VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: INTERNATIONALE RECHERCHENBEHÖRDE

PCT

MITTEILUNG ÜBER DIE ÜBERMITTLUNG DES INTERNATIONALEN RECHERCHENBERICHTS ODER DER ERKLÄRUNG

(Regel 44.1 PCT)

An
SCHOPPE, ZIMMERMANN & STÖCKELER
z.H. SCHOPPE, FRITZ
Postfach 71 08 67
81458 München
GERMANY

	Absendedatum *(Tag/Monat/Jahr)* 07/09/2000
Aktenzeichen des Anmelders oder Anwalts FH991204.PCT	**WEITERES VORGEHEN** siehe Punkte 1 und 4 unten
Internationales Aktenzeichen PCT/EP 99/09977	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 15/12/1999
Anmelder FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG...et al.	

1. [X] Dem Anmelder wird mitgeteilt, daß der internationale Recherchenbericht erstellt wurde und ihm hiermit übermittelt wird.

Einreichung von Änderungen und einer Erklärung nach Artikel 19:
Der Anmelder kann auf eigenen Wunsch die Ansprüche der internationalen Anmeldung ändern (siehe Regel 46):

Bis wann sind Änderungen einzureichen?

Die Frist zur Einreichung solcher Änderungen beträgt üblicherweise zwei Monate ab der Übermittlung des internationalen Recherchenberichts; weitere Einzelheiten sind den Anmerkungen auf dem Beiblatt zu entnehmen.

Wo sind Änderungen einzureichen?

Unmittelbar beim Internationalen Büro der WIPO, 34, CHEMIN des Colombettes, CH-1211 Genf 20, Telefaxnr.: (41-22) 740.14.35

Nähere Hinweise sind den Anmerkungen auf dem Beiblatt zu entnehmen.

2. [ ] Dem Anmelder wird mitgeteilt, daß kein internationaler Recherchenbericht erstellt wird und daß ihm hiermit die Erklärung nach Artikel 17(2)a) übermittelt wird.

3. [ ] **Hinsichtlich des Widerspruchs** gegen die Entrichtung einer zusätzlichen Gebühr (zusätzlicher Gebühren) nach Regel 40.2 wird dem Anmelder mitgeteilt, daß

[ ] der Widerspruch und die Entscheidung hierüber zusammen mit seinem Antrag auf Übermittlung des Wortlauts sowohl des Widerspruchs als auch der Entscheidung hierüber an die Bestimmungsämter dem Internationalen Büro übermittelt worden sind.

[ ] noch keine Entscheidung über den Widerspruch vorliegt; der Anmelder wird benachrichtigt, sobald eine Entscheidung getroffen wurde.

4. **Weiteres Vorgehen:** Der Anmelder wird auf folgendes aufmerksam gemacht:

Kurz nach Ablauf von **18 Monaten** seit dem Prioritätsdatum wird die internationale Anmeldung vom Internationalen Büro veröffentlicht. Will der Anmelder die Veröffentlichung verhindern oder auf einen späteren Zeitpunkt verschieben, so muß gemäß Regel 90bis.1 bzw. 90bis.3 vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung eine Erklärung über die Zurücknahme der internationalen Anmeldung oder des Prioritätsanspruchs beim Internationalen Büro eingehen.

Innerhalb von **19 Monaten** seit dem Prioritätsdatum ist ein Antrag auf internationale vorläufige Prüfung einzureichen, wenn der Anmelder den Eintritt in die nationale Phase bis zu 30 Monaten seit dem Prioritätsdatum (in manchen Ämtern sogar noch länger) verschieben möchte.

Innerhalb von **20 Monaten** seit dem Prioritätsdatum muß der Anmelder die für den Eintritt in die nationale Phase vorgeschriebenen Handlungen vor allen Bestimmungsämtern vornehmen, die nicht innerhalb von 19 Monaten seit dem Prioritätsdatum in der Anmeldung oder einer nachträglichen Auswahlerklärung ausgewählt wurden oder nicht ausgewählt werden konnten, da für sie Kapitel II des Vertrages nicht verbindlich ist.

Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bevollmächtigter Bediensteter Carole Emery

(Siehe Anmerkungen auf Beiblatt)

ANMERKUNGEN ZU FORMBLATT PCT/ISA/220

Diese Anmerkungen sollen grundlegende Hinweise zur Einreichung von Änderungen gemäß Artikel 19 geben. Diesen Anmerkungen liegen die Erfordernisse des Vertrags über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens (PCT), der Ausführungsordnung und der Verwaltungsrichtlinien zu diesem Vertrag zugrunde. Bei Abweichungen zwischen diesen Anmerkungen und obengenannten Texten sind letztere maßgebend. Nähere Einzelheiten sind dem PCT-Leitfaden für Anmelder, einer Veröffentlichung der WIPO, zu entnehmen.
Die in diesen Anmerkungen verwendeten Begriffe "Artikel", "Regel" und "Abschnitt" beziehen sich jeweils auf die Bestimmungen des PCT-Vertrags, der PCT-Ausführungsordnung bzw. der PCT-Verwaltungsrichtlinien.

HINWEISE ZU ÄNDERUNGEN GEMÄSS ARTIKEL 19

Nach Erhalt des internationalen Recherchenberichts hat der Anmelder die Möglichkeit, einmal die Ansprüche der internationalen Anmeldung zu ändern. Es ist jedoch zu betonen, daß, da alle Teile der internationalen Anmeldung (Ansprüche, Beschreibung und Zeichnungen) während des internationalen vorläufigen Prüfungsverfahrens geändert werden können, normalerweise keine Notwendigkeit besteht, Änderungen der Ansprüche nach Artikel 19 einzureichen, außer wenn der Anmelder z.B. zum Zwecke eines vorläufigen Schutzes die Veröffentlichung dieser Anspruche wünscht oder ein anderer Grund für eine Änderung der Ansprüche vor ihrer internationalen Veröffentlichung vorliegt. Weiterhin ist zu beachten, daß ein vorläufiger Schutz nur in einigen Staaten erhältlich ist.

Welche Teile der internationalen Anmeldung können geändert werden?

Im Rahmen von Artikel 19 können nur die Ansprüche geändert werden.

In der internationalen Phase können die Ansprüche auch nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert (oder nochmals geändert) werden. Die Beschreibung und die Zeichnungen können nur nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert werden.

Beim Eintritt in die nationale Phase können alle Teile der internationalen Anmeldung nach Artikel 28 oder gegebenenfalls Artikel 41 geändert werden.

Bis wann sind Änderungen einzureichen?

Innerhalb von zwei Monaten ab der Übermittlung des internationalen Recherchenberichts oder innerhalb von sechzehn Monaten ab dem Prioritätsdatum, je nachdem, welche Frist später abläuft. Die Änderungen gelten jedoch als rechtzeitig eingereicht, wenn sie dem Internationalen Büro nach Ablauf der maßgebenden Frist, aber noch vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung (Regel 46.1) zugehen.

Wo sind die Änderungen nicht einzureichen?

Die Änderungen können nur beim Internationalen Büro, nicht aber beim Anmeldeamt oder der Internationalen Recherchenbehörde eingereicht werden (Regel 46.2).

Falls ein Antrag auf internationale vorläufige Prüfung eingereicht wurde/wird, siehe unten.

In welcher Form können Änderungen erfolgen?

Eine Änderung kann erfolgen durch Streichung eines oder mehrerer ganzer Ansprüche, durch Hinzufügung eines oder mehrerer neuer Ansprüche oder durch Änderung des Wortlauts eines oder mehrerer Ansprüche in der eingereichten Fassung.

Für jedes Anspruchsblatt, das sich aufgrund einer oder mehrerer Änderungen von dem ursprünglich eingereichten Blatt unterscheidet, ist ein Ersatzblatt einzureichen.

Alle Ansprüche, die auf einem Ersatzblatt erscheinen, sind mit arabischen Ziffern zu numerieren. Wird ein Anspruch gestrichen, so brauchen, die anderen Ansprüche nicht neu numeriert zu werden. Im Fall einer Neunumerierung sind die Ansprüche fortlaufend zu numerieren (Verwaltungsrichtlinien, Abschnitt 205 b)).

Die Änderungen sind in der Sprache abzufassen, in der dieinternationale Anmeldung veröffentlicht wird.

Welche Unterlagen sind den Änderungen beizufügen?

Begleitschreiben (Abschnitt 205 b)):

Die Änderungen sind mit einem Begleitschreiben einzureichen.

Das Begleitschreiben wird nicht zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht. Es ist nicht zu verwechseln mit der "Erklärung nach Artikel 19(1)" (siehe unten, "Erklärung nach Artikel 19 (1)").

Das Begleitschreiben ist nach Wahl des Anmelders in englischer oder französischer Sprache abzufassen. Bei englischsprachigen internationalen Anmeldungen ist das Begleitschreiben aber ebenfalls in englischer, bei französischsprachigen internationalen Anmeldungen in französischer Sprache abzufassen.

ANMERKUNGEN ZU FORMBLATT PCT/ISA/220 (Fortsetzung)

Im Begleitschreiben sind die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen anzugeben. So ist insbesondere zu jedem Anspruch in der internationalen Anmeldung anzugeben (gleichlautende Angaben zu verschiedenen Ansprüchen können zusammengefaßt werden), ob

i) der Anspruch unverändert ist;

ii) der Anspruch gestrichen worden ist;

iii) der Anspruch neu ist;

iv) der Anspruch einen oder mehrere Ansprüche in der eingereichten Fassung ersetzt;

v) der Anspruch auf die Teilung eines Anspruchs in der eingereichten Fassung zurückzuführen ist.

Im folgenden sind Beispiele angegeben, wie Änderungen im Begleitschreiben zu erläutern sind:

1. [Wenn anstelle von ursprünglich 48 Ansprüchen nach der Änderung einiger Ansprüche 51 Ansprüche existieren]:
"Die Ansprüche 1 bis 29, 31, 32, 34, 35, 37 bis 48 werden durch geänderte Ansprüche gleicher Numerierung ersetzt; Ansprüche 30, 33 und 36 unverändert; neue Ansprüche 49 bis 51 hinzugefügt."

2. [Wenn anstelle von ursprünglich 15 Ansprüchen nach der Änderung aller Ansprüche 11 Ansprüche existieren]:
"Geänderte Ansprüche 1 bis 11 treten an die Stelle der Ansprüche 1 bis 15."

3. [Wenn ursprünglich 14 Ansprüche existierten und die Änderungen darin bestehen, daß einige Ansprüche gestrichen werden und neue Ansprüche hinzugefügt werden]:
Ansprüche 1 bis 6 und 14 unverändert; Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt."Oder" Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt; alle übrigen Ansprüche unverändert."

4. [Wenn verschiedene Arten von Änderungen durchgeführt werden]:
"Ansprüche 1-10 unverändert; Ansprüche 11 bis 13, 18 und 19 gestrichen; Ansprüche 14, 15 und 16 durch geänderten Anspruch 14 ersetzt; Anspruch 17 in geänderte Ansprüche 15, 16 und 17 unterteilt; neue Ansprüche 20 und 21 hinzugefügt."

"Erklärung nach Artikel 19(1)" (Regel 46.4)

Den Änderungen kann eine Erklärung beigefügt werden, mit der die Änderungen erläutert und ihre Auswirkungen auf die Beschreibung und die Zeichnungen dargelegt werden (die nicht nach Artikel 19 (1) geändert werden können).

Die Erklärung wird zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht.

Sie ist in der Sprache abzufassen, in der die internationale Anmeldung veröffentlicht wird.

Sie muß kurz gehalten sein und darf, wenn in englischer Sprache abgefaßt oder ins Englische übersetzt, nicht mehr als 500 Wörter umfassen

Die Erklärung ist nicht zu verwechseln mit dem Begleitschreiben, das auf die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen hinweist, und ersetzt letzteres nicht. Sie ist auf einem gesonderten Blatt einzureichen und in der Überschrift als solche zu kennzeichnen, vorzugsweise mit den Worten "Erklärung nach Artikel 19 (1)".

Die Erklärung darf keine herabsetzenden Äußerungen über den internationalen Recherchenbericht oder die Bedeutung von in dem Bericht angeführten Veröffentlichungen enthalten. Sie darf auf im internationalen Recherchenbericht angeführte Veröffentlichungen, die sich auf einen bestimmten Anspruch beziehen, nur im Zusammenhang mit einer Änderung dieses Anspruchs Bezug nehmen.

Auswirkungen eines bereits gestellten Antrags auf internationale vorläufige Prüfung

Ist zum Zeitpunkt der Einreichung von Änderungen nach Artikel 19 bereits ein Antrag auf internationale vorläufige Prüfung gestellt worden, so sollte der Anmelder in seinem Interesse gleichzeitig mit der Einreichung der Änderungen beim Internationalen Büro auch eine Kopie der Änderungen bei der mit der internationalen vorläufigen Prüfung beauftragen Behörde einreichen (siehe Regel 62.2 a), erster Satz).

Auswirkungen von Änderungen hinsichtlich der Übersetzung der internationalen Anmeldung beim Eintritt in die nationale Phase

Der Anmelder wird darauf hingewiesen, daß bei Eintritt in die nationale Phase möglicherweise anstatt oder zusätzlich zu der Übersetzung der Ansprüche in der eingereichten Fassung eine Übersetzung der nach Artikel 19 geänderten Ansprüche an die bestimmten/ausgewählten Ämter zu übermitteln ist.

Nähere Einzelheiten über die Erfordernisse jedes bestimmten/ausgewählten Amts sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
FH991204.PCT		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/EP 99/ 09977	15/12/1999	16/02/1999
Anmelder		
FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG...et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

   [X] wie vom Anmelder vorgeschlagen [ ] keine der Abb.

   [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 99/09977

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04N7/16 H04H1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04H

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 860 823 A (TOKYO SHIBAURA ELECTRIC CO) 26. August 1998 (1998-08-26) Seite 2, Zeile 1 -Seite 7, Zeile 51; Ansprüche 1,2; Abbildung 3 ---	1,6,12, 13
A	EP 0 717 564 A (LG ELECTRONICS INC) 19. Juni 1996 (1996-06-19) Spalte 1, Zeile 1 -Spalte 3, Zeile 43; Ansprüche 1,9 ---	1,6,12, 13
A	EP 0 874 503 A (SONY CORP) 28. Oktober 1998 (1998-10-28) Spalte 1, Zeile 1 -Spalte 2, Zeile 56; Anspruch 1; Abbildung 3 ---	1,6,12, 13

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
31. August 2000	07/09/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	De Haan, A.J.

4

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

Internationales Aktenzeichen
P[redacted]P 99/09977

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 5 303 303 A (WHITE ANDREW R) 12. April 1994 (1994-04-12) Spalte 1, Zeile 1 -Spalte 2, Zeile 60; Anspruch 1	1,6,12, 13
A	US 5 689 566 A (NGUYEN MINHTAM C) 18. November 1997 (1997-11-18) Spalte 1, Zeile 1 -Spalte 2, Zeile 3; Ansprüche 1,5	1,6,12, 13
A	US 5 559 814 A (ROLIN PIERRE ET AL) 24. September 1996 (1996-09-24) Spalte 1, Zeile 1 -Spalte 3, Zeile 67; Anspruch 1	1,6,12, 13
A	EP 0 755 056 A (AT & T CORP) 22. Januar 1997 (1997-01-22) Spalte 1, Zeile 1 -Spalte 2, Zeile 15; Anspruch 1	1,6,12, 13

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die [redacted]iben Patentfamilie gehören

Inte[redacted]ales Aktenzeichen
P[redacted]P 99/09977

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP 0860823	A	26-08-1998	JP	3020613 B	15-03-2000
			US	5987126 A	16-11-1999
			WO	9802881 A	22-01-1998
EP 0717564	A	19-06-1996	KR	152788 B	15-10-1998
			CN	1131528 A	25-09-1996
			CN	1150737 A	28-05-1997
			JP	2824231 B	11-11-1998
			JP	8252200 A	01-10-1996
			JP	2898591 B	02-06-1999
			JP	8273299 A	18-10-1996
			US	6028932 A	22-02-2000
			US	5761302 A	02-06-1998
EP 0874503	A	28-10-1998	JP	10303945 A	13-11-1998
US 5303303	A	12-04-1994	AU	8232091 A	18-02-1992
			WO	9202095 A	06-02-1992
			GB	2248535 A,B	08-04-1992
			PT	98359 A	31-08-1993
US 5689566	A	18-11-1997	US	5638448 A	10-06-1997
US 5559814	A	24-09-1996	FR	2717334 A	15-09-1995
			EP	0676881 A	11-10-1995
EP 0755056	A	22-01-1997	US	5670730 A	23-09-1997
			CA	2176982 A	23-11-1996
			JP	9022589 A	21-01-1997

T 5

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)
FH991204PCT		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/EP99/09977	15/12/1999	16/02/1999
Internationale Patentklassification (IPK) oder nationale Klassifikation und IPK		
H04N7/16		
Anmelder		
FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG...et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 6 Blätter einschließlich dieses Deckblatts.

   ☐ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☒ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
13/09/2000	17.11.2000
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:	Bevollmächtigter Bediensteter
Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Loeser, E Tel. Nr. +49 89 2399 8482

Formblatt PCT/IPEA/409 (Deckblatt) (Januar 1994)

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP99/09977

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten.*):
Beschreibung, Seiten:

1-19 ursprüngliche Fassung

Patentansprüche, Nr.:

1-17 ursprüngliche Fassung

Zeichnungen, Blätter:

1-4 ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

   Die Bestandteile standen Behörde in der Sprache: , zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
   ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

   ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
   ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
   ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
   ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
   ☐ Die Erklärung, dass das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
   ☐ Die Erklärung, dass die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung, Seiten:
- ☐ Ansprüche, Nr.:
- ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

   (Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen;sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-17
	Nein:	Ansprüche	
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	1-17
	Nein:	Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1-17
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen
   siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:
siehe Beiblatt

1. Betr. Abschnitt V - Artikel 33 PCT

1.1. Anspruch 1

Es wird auf die folgenden Dokumente Bezug genommen:

D1: DE-C-19 625 635;

D2: US-A-5 303 303.

D1 wurde im internationalen Recherchenbericht nicht angegeben, ist jedoch in der Beschreibung der vorliegenden Anmeldung (S.2) zitiert und zusammengefaßt.

Gemäß D1 war es vorbekannt, einen verschlüsselten Multimedia-Datenstrom zu erzeugen, bei welchem auf einen Bestimmungsdatenblock (Anfangsblock bzw. Header) ein Nutzdatenblock folgt, der zumindest teilweise verschlüsselt ist (D1: Fig.3).

Gemäß vorliegendem Anspruch 1 ist ebenfalls vorgesehen, einen Header (Anfangsblock (12)) zu erzeugen. Die Position des Headers im Datenstrom ist jedoch nicht festgelegt, schließt jedoch die aus D1 vorbekannte Position am Anfang des Datenstromes ein. Somit ist dieses beanspruchte Merkmal nicht neu.

Es wird angemerkt, daß D2 (Zusammenfassung; Fig.1) neben einem Header am Anfang einen weiteren Header am Ende eines Datenstromes offenbart. Daraus würde der Fachmann schließen, daß Header-Information nicht nur am Anfang sondern auch an anderer Stelle in den Datenstrom eingefügt werden kann. Insoweit könnte dem beanspruchten Merkmal eine erfinderische Tätigkeit nicht zugeordnet werden, selbst wenn es neu gegenüber D1 wäre.

Gemäß vorliegendem Anspruch 1 ist ferner vorgesehen, wie in D1 oder D2 einen Nutzdatenblock zu erzeugen. Laut Anspruch 1 geht einem verschlüsselten zweiten Teil des Nutzdatenblocks ein

unverschlüsselter erster Teil voraus.

Zweck dieses Verfahren ist es, bei der Entschlüsselung von Multimedia-Dateien sowohl eine Vorschau-Funktion zu erhalten als auch ein sofortiges Abspielen mit geringem apparativem Aufwand zu ermöglichen.

Effektiv ist somit gemäß Anspruch 1 der Nutzdatenblock nur teilweise verschlüsselt, wie aus D1 vorbekannt. D1 offenbart jedoch nicht, den unverschlüsselten Teil dem verschlüsselten Teil vorausgehen zu lassen. D1 schlägt lediglich vor, eine teilweise Verschlüsselung vorzunehmen und zeigt dazu (D1: Fig.3), den unverschlüsselten Teil auf den verschlüsselten folgen zu lassen.

Im Lichte der Offenbarung von D1 könnte der Fachmann zwar auch eine Anordnung in der umgekehrten Reihenfolgen (unverschlüsselt vor verschlüsselt), also wie beansprucht, in Betracht ziehen. Er hätte jedoch keinerlei Veranlassung dazu, die in D1 explizit gezeigte Reihenfolge zu ändern. Zudem ist die von der vorliegenden Erfindung gelöste Aufgabe aus dem vorliegenden Stand der Technik weder bekannt noch ableitbar.

Aus diesen Gründen wird Anspruch 1 ein erfinderischer Schritt zuerkannt (Erfordernisse der Art. 33(2) und (3) erfüllt).

1.2. Anspruch 6

Anspruch 6 betrifft das Abspielen eines verschlüsselten Multimedia-Datenstromes, der mit dem Verfahren gemäß Anspruch 1 erzeugbar ist. Der speziellen Verfahrensmerkmale von Anspruch 6 beinhalten, daß

(a) vom Anfangsblock diejenigen Daten verarbeitet werden, die zum Anspielen des (unverschlüsselten) Anfangsabschnittes des Nutzdatenblocks erforderlich sind;
(b) der unverschlüsselte Anfangsabschnitt des Nutzdatenblocks

abgespielt wird.

Weder Merkmal (a) noch Merkmal (b) sind aus dem Stand der Technik (D1, D2) vorbekannt oder ableitbar.

Somit sind die Erfordernisse der Art. 33(2) und (3) erfüllt.

1.3. Ansprüche 12, 13

Die Vorrichtungsansprüche 12 und 13 korrespondieren mit den Ansprüchen 1 und 6, sodaß die Erfordernisse der Art. 33(2) und (3) ebenfalls erfüllt sind.

1.4.

Der Erfindungsgegenstand ist gewerblich anwendbar.

2. Betr. Abschnitt VII: Bemerkungen und formale Einwände

2.1.

Die unabhängigen Ansprüche sind nicht in der zweiteiligen Form nach Regel 6.3 b) PCT abgefaßt. Im vorliegenden Fall erscheint die Zweiteilung jedoch nicht zweckmäßig.

2.2.

Auf S.4 (Abs.5 Zeile 2) muß "Viedeodaten" korrekt "Videodaten" lauten.

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark Office, PCT
2011 South Clark Place Room CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 08 November 2000 (08.11.00)	
International application No. PCT/EP99/09977	**Applicant's or agent's file reference** FH991204.PCT
International filing date (day/month/year) 15 December 1999 (15.12.99)	**Priority date** (day/month/year) 16 February 1999 (16.02.99)
Applicant RUMP, Niels et al	

1. The designated Office is hereby notified of its election made:

   [X] in the demand filed with the International Preliminary Examining Authority on:

   13 September 2000 (13.09.00)

   [ ] in a notice effecting later election filed with the International Bureau on:

   _____

2. The election [X] was

   [ ] was not

   made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

S. Mafla

Telephone No.: (41-22) 338.83.38

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: MIT DER INTERNATIONALEN VORLÄUFIGEN PRÜFUNG BEAUFTRAGTE BEHÖRDE

An:

SCHOPPE, Fritz
SCHOPPE, ZIMMERMANN & STÖCKELER
Postfach 71 08 67
81458 München
ALLEMAGNE

EINGEGANGEN
20. NOV. 2000

PCT

MITTEILUNG ÜBER DIE ÜBERSENDUNG DES INTERNATIONALEN VORLÄUFIGEN PRÜFUNGSBERICHTS

(Regel 71.1 PCT)

Absendedatum *(Tag/Monat/Jahr)*	17.11.2000
Aktenzeichen des Anmelders oder Anwalts: FH991204PCT	**WICHTIGE MITTEILUNG**

Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/EP99/09977	15/12/1999	16/02/1999

Anmelder: FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG...et al.

1. Dem Anmelder wird mitgeteilt, daß ihm die mit der internationalen vorläufigen Prüfung beauftragte Behörde hiermit den zu der internationalen Anmeldung erstellten internationalen vorläufigen Prüfungsbericht, gegebenenfalls mit den dazugehörigen Anlagen, übermittelt.

2. Eine Kopie des Berichts wird - gegebenenfalls mit den dazugehörigen Anlagen - dem Internationalen Büro zur Weiterleitung an alle ausgewählten Ämter übermittelt.

3. Auf Wunsch eines ausgewählten Amts wird das Internationale Büro eine Übersetzung des Berichts (jedoch nicht der Anlagen) ins Englische anfertigen und diesem Amt übermitteln.

4. **ERINNERUNG**

   Zum Eintritt in die nationale Phase hat der Anmelder vor jedem ausgewählten Amt innerhalb von 30 Monaten ab dem Prioritätsdatum (oder in manchen Ämtern noch später) bestimmte Handlungen (Einreichung von Übersetzungen und Entrichtung nationaler Gebühren) vorzunehmen (Artikel 39 (1)) (siehe auch die durch das Internationale Büro im Formblatt PCT/IB/301 übermittelte Information).

   Ist einem ausgewählten Amt eine Übersetzung der internationalen Anmeldung zu übermitteln, so muß diese Übersetzung auch Übersetzungen aller Anlagen zum internationalen vorläufigen Prüfungsbericht enthalten. Es ist Aufgabe des Anmelders, solche Übersetzungen anzufertigen und den betroffenen ausgewählten Ämtern direkt zuzuleiten.

   Weitere Einzelheiten zu den maßgebenden Fristen und Erfordernissen der ausgewählten Ämter sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde
Europäisches Patentamt
D-80298 München
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Bevollmächtigter Bediensteter
SCHALINATUS, D
Tel. +49 89 2399-8242

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts	**WEITERES VORGEHEN**	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)
FH991204PCT		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/EP99/09977	15/12/1999	16/02/1999
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK		
H04N7/16		
Anmelder		
FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG...et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 6 Blätter einschließlich dieses Deckblatts.

   ☐ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☒ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
13/09/2000	17.11.2000
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:	Bevollmächtigter Bediensteter
Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Loeser, E Tel. Nr. +49 89 2399 8482

Formblatt PCT/IPEA/409 (Deckblatt) (Januar 1994)

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP99/09977

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten.*):
Beschreibung, Seiten:

1-19 ursprüngliche Fassung

Patentansprüche, Nr.:

1-17 ursprüngliche Fassung

Zeichnungen, Blätter:

1-4 ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

   Die Bestandteile standen Behörde in der Sprache: , zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
   ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

   ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
   ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
   ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
   ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
   ☐ Die Erklärung, dass das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
   ☐ Die Erklärung, dass die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung, Seiten:
- ☐ Ansprüche, Nr.:
- ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

   (Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen;sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-17
	Nein:	Ansprüche	
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	1-17
	Nein:	Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1-17
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen
   siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:
siehe Beiblatt

1. Betr. Abschnitt V - Artikel 33 PCT

1.1. Anspruch 1

Es wird auf die folgenden Dokumente Bezug genommen:

D1: DE-C-19 625 635;

D2: US-A-5 303 303.

D1 wurde im internationalen Recherchenbericht nicht angegeben, ist jedoch in der Beschreibung der vorliegenden Anmeldung (S.2) zitiert und zusammengefaßt.

Gemäß D1 war es vorbekannt, einen verschlüsselten Multimedia-Datenstrom zu erzeugen, bei welchem auf einen Bestimmungsdatenblock (Anfangsblock bzw. Header) ein Nutzdatenblock folgt, der zumindest teilweise verschlüsselt ist (D1: Fig.3).

Gemäß vorliegendem Anspruch 1 ist ebenfalls vorgesehen, einen Header (Anfangsblock (12)) zu erzeugen. Die Position des Headers im Datenstrom ist jedoch nicht festgelegt, schließt jedoch die aus D1 vorbekannte Position am Anfang des Datenstromes ein. Somit ist dieses beanspruchte Merkmal nicht neu.

Es wird angemerkt, daß D2 (Zusammenfassung; Fig.1) neben einem Header am Anfang einen weiteren Header am Ende eines Datenstromes offenbart. Daraus würde der Fachmann schließen, daß Header-Information nicht nur am Anfang sondern auch an anderer Stelle in den Datenstrom eingefügt werden kann. Insoweit könnte dem beanspruchten Merkmal eine erfinderische Tätigkeit nicht zugeordnet werden, selbst wenn es neu gegenüber D1 wäre.

Gemäß vorliegendem Anspruch 1 ist ferner vorgesehen, wie in D1 oder D2 einen Nutzdatenblock zu erzeugen. Laut Anspruch 1 geht einem verschlüsselten zweiten Teil des Nutzdatenblocks ein

unverschlüsselter erster Teil voraus.

Zweck dieses Verfahren ist es, bei der Entschlüsselung von Multimedia-Dateien sowohl eine Vorschau-Funktion zu erhalten als auch ein sofortiges Abspielen mit geringem apparativem Aufwand zu ermöglichen.

Effektiv ist somit gemäß Anspruch 1 der Nutzdatenblock nur teilweise verschlüsselt, wie aus D1 vorbekannt. D1 offenbart jedoch nicht, den unverschlüsselten Teil dem verschlüsselten Teil vorausgehen zu lassen. D1 schlägt lediglich vor, eine teilweise Verschlüsselung vorzunehmen und zeigt dazu (D1: Fig.3), den unverschlüsselten Teil auf den verschlüsselten folgen zu lassen.

Im Lichte der Offenbarung von D1 könnte der Fachmann zwar auch eine Anordnung in der umgekehrten Reihenfolgen (unverschlüsselt vor verschlüsselt), also wie beansprucht, in Betracht ziehen. Er hätte jedoch keinerlei Veranlassung dazu, die in D1 explizit gezeigte Reihenfolge zu ändern. Zudem ist die von der vorliegenden Erfindung gelöste Aufgabe aus dem vorliegenden Stand der Technik weder bekannt noch ableitbar.

Aus diesen Gründen wird Anspruch 1 ein erfinderischer Schritt zuerkannt (Erfordernisse der Art. 33(2) und (3) erfüllt).

1.2. Anspruch 6

Anspruch 6 betrifft das Abspielen eines verschlüsselten Multimedia-Datenstromes, der mit dem Verfahren gemäß Anspruch 1 erzeugbar ist. Der speziellen Verfahrensmerkmale von Anspruch 6 beinhalten, daß

(a) vom Anfangsblock diejenigen Daten verarbeitet werden, die zum Anspielen des (unverschlüsselten) Anfangsabschnittes des Nutzdatenblocks erforderlich sind;
(b) der unverschlüsselte Anfangsabschnitt des Nutzdatenblocks

abgespielt wird.

Weder Merkmal (a) noch Merkmal (b) sind aus dem Stand der Technik (D1, D2) vorbekannt oder ableitbar.

Somit sind die Erfordernisse der Art. 33(2) und (3) erfüllt.

1.3. Ansprüche 12, 13

Die Vorrichtungsansprüche 12 und 13 korrespondieren mit den Ansprüchen 1 und 6, sodaß die Erfordernisse der Art. 33(2) und (3) ebenfalls erfüllt sind.

1.4.

Der Erfindungsgegenstand ist gewerblich anwendbar.

2. Betr. Abschnitt VII: Bemerkungen und formale Einwände

2.1.

Die unabhängigen Ansprüche sind nicht in der zweiteiligen Form nach Regel 6.3 b) PCT abgefaßt. Im vorliegenden Fall erscheint die Zweiteilung jedoch nicht zweckmäßig.

2.2.

Auf S.4 (Abs.5 Zeile 2) muß "Viedeodaten" korrekt "Videodaten" lauten.

FH991204.PCT

PCT-ANTRAG

Original (für EINREICHUNG) - gedruckt am 15.12.1999 11:34:35 AM

0 0-1	**Vom Anmeldeamt auszufüllen** Internationales Aktenzeichen.	
0-2	Internationales Anmeldedatum	
0-3	Name des Anmeldeamts und "PCT International Application"	

0-4 0-4-1	**Formular - PCT/RO/101 PCT-Antrag** erstellt durch Benutzung von	PCT-EASY Version 2.90 (aktualisiert 15.10.1999)
0-5	**Antragsersuchen** Der Unterzeichnete beantragt, daß die vorliegende internationale Anmeldung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens behandelt wird	
0-6	**(Vom Anmelder gewähltes) Anmeldeamt**	Europäisches Patentamt (EPA) (RO/EP)
0-7	**Aktenzeichen des Anmelders oder Anwalts**	FH991204.PCT
I	**Bezeichnung der Erfindung**	VERFAHREN UND VORRICHTUNG ZUM ERZEUGEN EINES VERSCHLÜSSELTEN NUTZDATENSTROMS UND VERFAHREN UND VORRICHTUNG ZUM ABSPIELEN EINES VERSCHLÜSSELTEN NUTZDATENSTROMS
II	**Anmelder**	
II-1	Diese Person ist	nur Anmelder
II-2	Anmelder für	Alle Bestimmungsstaaten mit Ausnahme von US
II-4	Name	FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
II-5	Anschrift:	Leonrodstraße 54 D-80636 München Deutschland
II-6	Staatsangehörigkeit (Staat)	DE
II-7	Sitz/Wohnsitz (Staat)	DE
III-1	**Anmelder und/oder Erfinder**	
III-1-1	Diese Person ist	Anmelder und Erfinder
III-1-2	Anmelder für	Nur US
III-1-4	Name (FAMILIENNAME, Vorname)	RUMP, Niels
III-1-5	Anschrift:	Brückenstraße 13 D-91056 Erlangen Deutschland
III-1-6	Staatsangehörigkeit (Staat)	DE
III-1-7	Sitz/Wohnsitz (Staat)	DE

PCT-ANTRAG

Original (für **EINREICHUNG**) - gedruckt am 15.12.1999 11:34:35 AM

III-2	**Anmelder und/oder Erfinder**	
III-2-1	Diese Person ist	Anmelder und Erfinder
III-2-2	Anmelder für	Nur US
III-2-4	Name (FAMILIENNAME, Vorname)	KOLLER, Jürgen
III-2-5	Anschrift:	St. Johann 6/113 D-91054 Erlangen Deutschland
III-2-6	Staatsangehörigkeit (Staat)	DE
III-2-7	Sitz/Wohnsitz (Staat)	DE
III-3	**Anmelder und/oder Erfinder**	
III-3-1	Diese Person ist	Anmelder und Erfinder
III-3-2	Anmelder für	Nur US
III-3-4	Name (FAMILIENNAME, Vorname)	BRANDENBURG, Karlheinz
III-3-5	Anschrift:	Haagstraße 32 D-91054 Erlangen Deutschland
III-3-6	Staatsangehörigkeit (Staat)	DE
III-3-7	Sitz/Wohnsitz (Staat)	DE
IV-1	**Anwalt oder gemeinsamer Vertreter; oder besondere Zustellanschrift** Die unten bezeichnete Person ist/wird hiermit bestellt, um den (die) Anmelder vor den internationalen Behörden zu vertreten, und zwar als:	Anwalt
IV-1-1	Name (FAMILIENNAME, Vorname)	SCHOPPE, Fritz
IV-1-2	Anschrift:	SCHOPPE, ZIMMERMANN & STÖCKELER POSTFACH 71 08 67 D-81458 München Deutschland
IV-1-3	Telefonnr.	089/7904450
IV-1-4	Telefaxnr.	089/7902215
IV-1-5	e-mail	101345.3117@CompuServe.com
V	**Bestimmung von Staaten**	
V-1	Regionales Patent (andere Schutzrechtsarten oder Verfahren sind ggf. in Klammern nach der (den) betreffenden Bestimmung(en) angegeben)	EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE und jeder weitere Staat, der Mitgliedsstaat des Europäischen Patentübereinkommens und Vertragsstaat des PCT ist
V-2	Nationales Patent (andere Schutzrechtsarten oder Verfahren sind ggf. in Klammern nach der (den) betreffenden Bestimmung(en) angegeben)	JP KR US

FH991204.PCT

PCT-ANTRAG

Original (für **EINREICHUNG**) - gedruckt am 15.12.1999 11:34:35 AM

V-5	**Erklärung bzgl. vorsorglicher Bestimmungen** Zusätzlich zu den unter Punkten V-1, V-2 and V-3 vorgenommenen Bestimmungen nimmt der Anmelder nach Regel 4.9 Absatz b auch alle anderen nach dem PCT zulässigen Bestimmungen vor mit Ausnahme der nachstehend unter Punkt V-6 angegebenen Staaten. Der Anmelder erklärt, daß diese zusätzlichen Bestimmungen unter dem Vorbehalt einer Bestätigung stehen und jede zusätzliche Bestimmung, die vor Ablauf von 15 Monaten ab dem Prioritätsdatum nicht bestätigt wurde, nach Ablauf dieser Frist als vom Anmelder zurückgenommen gilt.		
V-6	**Staaten, die von der Erklärung über vorsorgliche Bestimmungen ausgenommen werden**	KEINE	
VI-1	**Priorität einer früheren nationalen Anmeldung beansprucht**		
VI-1-1	Anmeldedatum	16 Februar 1999 (16.02.1999)	
VI-1-2	Aktenzeichen	19906449.0	
VI-1-3	Staat	DE	
VII-1	**Gewählte Internationale Recherchenbehörde**	Europäisches Patentamt (EPA) (ISA/EP)	
VIII	**Kontrolliste**	Anzahl der Blätter	Elektronische Datei(en) beigefügt
VIII-1	Antrag	4	-
VIII-2	Beschreibung	19	-
VIII-3	Ansprüche	6	-
VIII-4	Zusammenfassung	1	fh991204.txt
VIII-5	Zeichnung(en)	4	-
VIII-7	INSGESAMT	34	
	Beigefügte Unterlagen	Unterlage(n) in Papierform beigefügt	Elektronische Datei(en) beigefügt
VIII-8	Blatt für die Gebührenberechnung	✓	-
VIII-10	Kopie der allgemeinen Vollmacht	Aktenzeichen 17406	-
VIII-16	PCT-EASY-Diskette	-	Diskette
VIII-18	**Nr. der Abb. der Zeichn., die mit der Zusammenf. veröffentlicht werden soll**	1	
VIII-19	**Sprache der Int. Anmeldung**	Deutsch	
IX-1	**Unterschrift des Anmelders oder Anwalts**		
IX-1-1	Name (FAMILIENNAME, Vorname)	SCHOPPE, Fritz	

VOM ANMELDEAMT AUSZUFÜLLEN

10-1	**Datum des tatsächlichen Eingangs dieser internationalen Anmeldung**	
10-2	**Zeichnung(en):**	
10-2-1	Eingegangen	
10-2-2	Nicht eingegangen	

PCT-ANTRAG

Original (für **EINREICHUNG**) - gedruckt am 15.12.1999 11:34:35 AM

10-3	Geändertes Eingangsdatum aufgrund nachträglich, jedoch fristgerecht eingeg. Unterlage(n) oder Zeichnung(en) zur Vervollständigung dieser int. Anmeldung	
10-4	Datum des fristgerechten Eingangs der Berichtigung nach PCT Artikel 11(2)	
10-5	Internationale Recherchenbehörde	ISA/EP
10-6	Übermittlung des Recherchenexemplars bis zur Zahlung der Recherchengebühr aufgeschoben	

VOM INTERNATIONALEN BÜRO AUSZUFÜLLEN

11-1	Datum des Eingangs des Aktenexemplars beim Internationalen Büro	

PCT

FH991204.PCT

Original (für **EINREICHUNG**) - gedruckt am 15.12.1999 11:34:35 AM

PCT-EASY-Informationsblatt

(Vom Anmelder auszufüllen; dieses Blatt NICHT mit der internationalen Anmeldung einreichen)

PRÜFPROTOKOLL

	Antrag
Grün?	Die Bezeichnung der Erfindung muß kurz und genau gefaßt sein. Bitte überprüfen.
	Staaten
Grün?	Es können mehr Bestimmungen vorgenommen werden. Bitte überprüfen.
	Namen
Grün?	Anmelder 1.: Telefonnr. nicht angegeben
Grün?	Anmelder 1.:Telefaxnr. nicht angegeben
	Inhalt
Grün?	Priority 1: der Prioritätsbeleg ist nicht beigefügt (der Anmelder muß ihn beim Anmeldeamt oder beim Internationalen Büro vor Ablauf von 16 Monaten ab dem (frühesten) Prioritätsdatum einreichen)
	Zahlung
Grün?	Bitte überprüfen Sie, daß bei dem gewählten Anmeldeamt ein gültiges laufendes Konto auf Ihren Namen besteht

Vor Einreichung der internationalen Anmeldung, bitte sorgfältig prüfen daß:

-die Angaben auf dem ausgedruckten Anmeldeformular sind richtig;
-Box IX of the Request form and item 12-22 of the Annex to the Request form have been signed;
-alle in Feld Nr. VIII des Antragsformulars angegebenen Bestandteile der internationalen Anmeldung sind beigefügt; und,
-die Diskette mit der PCT-EASY-Zipdatei der internationalen Anmeldung ist beigefügt und eindeutig mit "PCT-EASY", dem Aktenzeichen des Anmelders/Anwalts und dem Familiennamen des Anmelders beschriftet

ACHTUNG

KEINE Angaben auf dem ausgedruckten Antragsformular verändern. Die beigefügte PCT-EASY-Anmeldung ist gesperrt. Falls jetzt ein Fehler oder eine Auslassung entdeckt wird, muß die eingereichte Anmeldung als Vorlage kopiert und die Änderung oder Berichtigung in einer neuen Anmeldung vorgenommen werden (unter Verwendung der Vorlage) Sie können eine solche Vorlage erstellen, indem Sie die eingereichte Anmeldung aus dem Ordner "Gespeicherte Formulare" in den Ordner "Neue PCT Formulare" kopieren. Neue, in dem Ordner "Neue PCT Formulare" erstellte (.eft) Datei öffnen, Berichtigungen vornehmen und das Einreichungsverfahren fortsetzen

FH991204.PCT

PCT (ANHANG - BLATT FÜR DIE GEBÜHRENBERECHNUNG)

Original (für **EINREICHUNG**) - gedruckt am 15.12.1999 11:34:35 AM

(Dieses Blatt zählt nicht als Blatt der internationalen Anmeldung und ist nicht Teil derselben)

0 0-1	**Vom Anmeldeamt auszufüllen** Internationales Aktenzeichen.				
0-2	Eingangsstempel des Anmeldeamts				
0-4 0-4-1	**Formular - PCT/RO/101 (Anlage) PCT Blatt für die Gebührenberechnung** erstellt durch Benutzung von	PCT-EASY Version 2.90 (aktualisiert 15.10.1999)			
0-9	**Aktenzeichen des Anmelders oder Anwalts**	FH991204.PCT			
2	**Anmelder**	FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V., et al.			
12	**Berechnung der vorgeschriebenen Gebühren**		Höhe der Gebühr/Multiplikator	Gesamtbeträge (EUR)	
12-1	Übermittlungsgebühr	T	⇨	102	
12-2	Recherchengebühr	S	⇨	945	
12-3	Internationale Gebühr Grundgebühr (erste 30 Blätter)	b1	413		
12-4	Anzahl der Blätter über 30		4		
12-5	Zusatzblattgebühr	(X)	10		
12-6	Gesamtbetrag der weiteren Gebühren	b2	40		
12-7	b1 + b2 =	B	453		
12-8	Bestimmungsgebühren Anzahl der in der internationalen Anmeldung vorgenommenen Bestimmungen		4		
12-9	Anzahl der zu zahlenden Bestimmungsgebühren (höchstens 10)		4		
12-10	Bestimmungsgebühr	(X)	95		
12-11	Gesamtbetrag der Bestimmungsgebühren	D	380		
12-12	PCT-EASY-Gebührenermäßigung	R	-127		
12-13	Gesamtbetrag der internationalen Gebühr (B+D-R)	I	⇨	706	
12-17	**Gesamtbetrag der zu zahlenden Gebühren (T+S+I+P)**		⇨	1.753	
12-19	**Zahlungsart**		Abbuchungsauftrag		
12-20	**Anweisungen betreffend laufendes Konto** Das Anmeldeamt:		Europäisches Patentamt (EPA) (RO/EP)		
12-20-1	wird beauftragt, den vorstehend angegebenen Gesamtbetrag der Gebühren von meinem laufenden Konto abzubuchen		✓		

FH991204.PCT

PCT (ANHANG - BLATT FÜR DIE GEBÜHRENBERECHNUNG)

Original (für **EINREICHUNG**) - gedruckt am 15.12.1999 11:34:35 AM

12-20-2	wird beauftragt, Fehlbeträge oder Überzahlungen des vorstehend angegebenen Gesamtbetrags der Gebühren meinem laufenden Konto zu belasten bzw. gutzuschreiben	✓
12-21	Nummer des laufenden Kontos	2800 0601
12-22	Datum	15 Dezember 1999 (15.12.1999)
12-23	Name und Unterschrift	SCHOPPE, Fritz

PRÜFPROTOKOLL UND BEMERKUNGEN

13-2-1	Prüfergebnisse Antrag	Grün? Die Bezeichnung der Erfindung muß kurz und genau gefaßt sein. Bitte überprüfen.
13-2-2	Prüfergebnisse Staaten	Grün? Es können mehr Bestimmungen vorgenommen werden. Bitte überprüfen.
13-2-3	Prüfergebnisse Namen	Grün? Anmelder 1.: Telefonnr. nicht angegeben
		Grün? Anmelder 1.:Telefaxnr. nicht angegeben
13-2-6	Prüfergebnisse Inhalt	Grün? Priority 1: der Prioritätsbeleg ist nicht beigefügt (der Anmelder muß ihn beim Anmeldeamt oder beim Internationalen Büro vor Ablauf von 16 Monaten ab dem (frühesten) Prioritätsdatum einreichen)
13-2-8	Prüfergebnisse Zahlung	Grün? Bitte überprüfen Sie, daß bei dem gewählten Anmeldeamt ein gültiges laufendes Konto auf Ihren Namen besteht

SCHOPPE, ZIMMERMANN & STÖCKELER

PATENTANWÄLTE

European Patent Attorneys
European Trademark Attorneys

Fritz Schoppe, Dipl.-Ing.
Tankred Zimmermann, Dipl.-Ing.
Ferdinand Stöckeler, Dipl.-Ing.

Telefon/Telephone 089/790445-0
Telefax/Facsimile 089/790 22 15
Telefax/Facsimile 089/74996977
e-mail 101345.3117@CompuServe.com

Patentanwälte · Postfach 710867 · 81458 München
Fraunhofer-Gesellschaft
zur Förderung der
angewandten Forschung e. V.
Leonrodstraße 54
D-80636 München
DE

Verfahren und Vorrichtung zum Erzeugen eines verschlüsselten Nutzdatenstroms und Verfahren und Vorrichtung zum Abspielen eines verschlüsselten Nutzdatenstroms

Verfahren und Vorrichtung zum Erzeugen eines verschlüsselten Nutzdatenstroms und Verfahren und Vorrichtung zum Abspielen eines verschlüsselten Nutzdatenstroms

Beschreibung

Die vorliegende Erfindung bezieht sich auf die Ver- bzw. Entschlüsselung von Nutzdaten und insbesondere auf die Handhabung von verschlüsselten Nutzdatenströmen, die einen Anfangsblock und einen Nutzdatenblock aufweisen.

Mit dem Auftreten von Telekommunikationsnetzen und insbesondere aufgrund der großen Verbreitung von Multimediadaten-fähigen Personalcomputern und in letzter Zeit auch von sogenannten Solid-State-Playern, entstand ein Bedarf, digitale Multimediadaten, wie z. B. digitale Audiodaten und/oder digitale Videodaten, kommerziell zu vertreiben. Die Telekommunikationsnetze können beispielsweise analoge Telephonleitungen, digitale Telephonleitungen, wie z. B. ISDN, oder auch das Internet sein. Unter kommerziellen Anbietern von Multimediaprodukten besteht der Bedarf, Multimediadaten zu verkaufen oder auszuleihen, wobei es einem Kunden möglich sein sollte, aus einem bestimmten Katalog zu jeder Zeit individuell ein bestimmtes Produkt auswählen zu können, das dann selbstverständlich nur von dem Kunden, der dafür bezahlt hat, benutzt werden darf.

Im Gegensatz zu bekannten verschlüsselten Fernsehprogrammen, wie z. B. von dem Fernsehkanal Premiere, bei dem die ausgesendeten Daten für alle Benutzer, die gegen eine bestimmte Gebühr eine geeignete Entschlüsselungsvorrichtung erworben haben, gleich verschlüsselt sind, soll die vorliegende Erfindung Verfahren und Vorrichtungen schaffen, die eine individuelle, kundenselektive und sichere Verschlüsselung und Entschlüsselung von Multimediadaten ermöglichen. Im Gegensatz zu den genannten Fernsehkanälen, die ein festes Programm vorgeben, für das sich der Benutzer komplett ent-

scheiden muß, ermöglichen die Verfahren und Vorrichtungen der vorliegenden Erfindung eine maximale Wahlfreiheit des Kunden, d. h. derselbe muß nur für die Produkte bezahlen, die er tatsächlich auch benutzen will.

Die DE 196 25 635 C1 beschreibt Verfahren und Vorrichtungen zum Ver- bzw. Entschlüsseln von Multimediadaten, wobei die Multimediadaten in Form einer verschlüsselten Multimediadatei vorliegen, die einen Bestimmungsdatenblock und einen Nutzdatenblock aufweist. Teile des Bestimmungsdatenblocks sowie zumindest Teile des Nutzdatenblocks werden mit unterschiedlichen Schlüsseln verschlüsselt, wobei insbesondere symmetrische Verschlüsselungsverfahren eingesetzt werden.

Symmetrische Verschlüsselungsverfahren haben einerseits den Vorteil, daß sie relativ schnell arbeiten, andererseits benötigt der Benutzer, der die Datei entschlüsseln will, den gleichen Schlüssel wie der Provider oder Lieferant, z. B. die Deutsche Telekom, der die Multimediadaten verschlüsselt hat, um sie an den Kunden zu verkaufen. Somit haben sowohl der Provider als auch der Benutzer, d. h. der Kunde, einerseits eine Tabelle mit vielen möglichen symmetrischen Verschlüsselungsalgorithmen, wie z. B. DES oder Blowfish, und andererseits eine Tabelle für mögliche Schlüssel, derart, daß vom Provider ein Eintrag in dem Bestimmungsdatenblock der Multimediadaten erzeugt wird, den der Benutzer verwendet, um damit auf seine Schlüsseltabelle zuzugreifen, um den korrekten Schlüssel zum Entschlüsseln auszuwählen.

Aufgrund der stark zunehmenden Verbreitung des MP3-Standards sind auf dem Markt sogenannten Solid-State-Player erschienen, die zum Entschlüsseln und Abspielen von Multimediadaten eingesetzt werden sollen. Diese Geräte sollen sehr preisgünstig sein und dürfen daher lediglich eine begrenzte Menge an Speicherplatz und Rechenleistung haben. Im Gegensatz zu Personalcomputern, bei denen die vorhandenen Ressourcen die für die Entschlüsselung von Multimediadaten benötigten Ressourcen bei weitem übersteigen, müssen Solid-State-Player

oder Stereoanlagen oder Auto-HiFi-Geräte, damit sie sich auf dem hart umkämpften Markt durchsetzen können, preiswert sein. Dazu ist es erforderlich, diese Geräte beim Entschlüsseln und Abspielen der entschlüsselten Multimediadaten soweit als möglich bezüglich Rechenleistung und Speicherplatz zu entlasten.

Nachteilig an dem in der DE 196 25 635 C1 beschriebenen Ver- bzw. Entschlüsselungskonzept ist die Tatsache, daß der gesamte Bestimmungsdatenblock vollständig verarbeitet werden muß, bevor mit dem Entschlüsseln des Nutzdatenblocks, dem Decodieren des entschlüsselten Nutzdatenblocks und schließlich dem Abspielen des entschlüsselten decodierten Nutzdatenblocks begonnen werden kann.

Dies wird besonders dann zum Problem, wenn die Verarbeitung des Bestimmungsdatenblocks in einer Entschlüsselungsvorrichtung aufwendigere Rechenoperationen mit sich bringt, wie beispielsweise die Berechnung einer Hash-Summe oder eines Fingerabdrucks des Anfangsblocks. Die Situation könnte noch dadurch verschärft werden, wenn die Entschlüsselungsvorrichtung über begrenzte Speicher- und Prozessorressourcen verfügt. Abspielgeräte insbesondere in Form eines Solid-State-Players sollen jedoch gerade begrenzte Speicher- und Prozessorressourcen haben, um preiswert auf dem Markt angeboten werden zu können.

Ein weiterer Nachteil des bekannten Ver- bzw. Entschlüsselungskonzepts ist die Tatsache, daß nicht ohne weiteres eine einfache Preview- bzw. Prelisten-Funktion möglich ist. Wenn es sich bei den Multimediadaten um Videodaten handelt, so ist es in bestimmten Fällen wünschenswert, die ersten beispielsweise 10 bis 20 Sekunden anzuschauen, um einerseits überhaupt erst eine Entscheidung zu treffen, das angebotene Stück zu kaufen, oder um andererseits ein bestimmtes Stück ohne weiteres identifizieren zu können. Handelt es sich bei den Multimediadaten um Audiodaten, so besteht der Bedarf, in ein Stück "reinzuhören", d. h. die ersten vielleicht 10 bis

20 Sekunden anzuhören, um dann zu entscheiden, ob das Stück gekauft werden soll, bzw. um das Stück zu identifizieren.

Die Aufgabe der vorliegenden Erfindung besteht darin, ein Konzept zum Erzeugen bzw. Abspielen von verschlüsselten Multimediadatenströmen zu schaffen, das mit mäßigen Speicher- und Prozessorressourcen auskommt und zugleich eine effiziente Implementation einer Preview- bzw. Prelisten-Funktion gestattet.

Diese Aufgabe wird durch ein Verfahren zum Erzeugen eines verschlüsselten Nutzdatenstroms nach Patentanspruch 1, durch ein Verfahren zum Abspielen eines verschlüsselten Nutzdatenstroms nach Patentanspruch 6, durch eine Vorrichtung zum Erzeugen eines verschlüsselten Nutzdatenstroms nach Patentanspruch 12 und durch eine Vorrichtung zum Abspielen eines verschlüsselten Nutzdatenstroms nach Patentanspruch 13 gelöst.

Der vorliegenden Erfindung liegt die Erkenntnis zugrunde, daß das Konzept verworfen werden muß, daß die Nutzdaten unmittelbar von Anfang an verschlüsselt werden. Im Stand der Technik bestand die Bestrebung immer, die Nutzdaten von Anfang an zu verschlüsseln, um das gesamte Nutzdatenstück und insbesondere den Anfang desselben vor unautorisierten Zugriffen zu schützen.

An dieser Stelle sei darauf hingewiesen, daß Nutzdaten allgemein Multimediadaten, d. h. Audiodaten, Viedeodaten oder eine Kombination aus Audiodaten und Videodaten, aber auch z. B. Textdaten umfassen. Im nachfolgenden wird der Gegenstand der vorliegenden Erfindung aus Zweckmäßigkeitsgünden jedoch anhand von Multimediadaten dargelegt. Es ist jedoch offensichtlich, daß sämtliche Nutzdaten, für die es ein Verschlüsselungsinteresse gibt, durch die erfindungsgemäßen Vorrichtungen und Verfahren verarbeitet werden können.

Es wurde jedoch herausgefunden, daß insbesondere dann, wenn

die Verarbeitung des Anfangsblocks komplexere Operationen, wie z. B. das Bilden von Hash-Summen, umfaßt, die Verzögerung, die durch die Verarbeitung des Anfangsblocks entsteht, signifikant werden kann, was insbesondere dann der Fall ist, wenn Abspielvorrichtungen mit begrenzten Speicher- und Prozessorressourcen verwendet werden sollen.

Ferner wurde herausgefunden, daß die Auslastung eines Prozessors mit begrenzter Prozessorleistung beim Verarbeiten des Anfangsblocks besonders hoch ist, während dieselbe beim Entschlüsseln, Decodieren und Abspielen der entschlüsselten decodierten Multimediadaten geringer ist. Dies bedeuet, daß lediglich für die Verarbeitung des Anfangsblocks relativ viel Prozessorleistung zur Verfügung gestellt werden muß, die dann beim Entschlüsseln, Decodieren und Abspielen des Datenstroms nicht mehr voll ausgenützt wird. Es sei darauf hingewiesen, daß die Sicherheit eines verschlüsselten Multimediadatenstroms im wesentlichen durch den Anfangsblock bestimmt wird, d. h., daß es immer sinnvoll ist, genau dort relativ viel Rechenleistung einzusetzen, um sichere Konzepte zu erhalten. Daher ist es nicht wünschenswert, die Verarbeitung des Anfangsblocks generell zu vereinfachen, um die Verzögerung des Verarbeitung des Anfangsblocks zu reduzieren.

Gemäß der vorliegenden Erfindung wird daher ein bestimmter Abschnitt, der am Beginn der zu verschlüsselnden Multimediadaten, d. h. am Beginn eines Nutzdatenblocks, startet und nach einer vorbestimmten Dauer der zu verschlüsselnden Multimediadaten endet, d. h. ein erster Teil der zu verschlüsselnden Multimediadaten, nicht verschlüsselt wird, sondern unverschlüsselt in einen Anfangsabschnitt des Nutzdatenblocks der verschlüsselten Multimediadatei geschrieben wird. Erst die Multimediadaten, die dem ersten Teil folgen, werden auf eine geeignete Art und Weise verschlüsselt und an den Anfangsabschnitt des Nutzdatenblocks angehängt. Dies bedeutet, daß der erste Teil eines Multimediadatenstücks, der sich üblicherweise in einem Bereich von 5 bis 20 Sekunden befinden dürfte, frei zugänglich ist. Um diesen ersten Teil

abzuspielen, sind die Prozessoranforderungen minimal, da keine Hash-Summen berechnet werden müssen, und da kein verschlüsselter Multimediadatenschlüssel entschlüsselt werden muß usw. Außerdem ist es in diesem Stadium nicht unbedingt erforderlich, ausgefeilte Lizenzdaten, die sich auf die erlaubte Verwendung des Multimediadatenstroms beziehen, zu verarbeiten. Ein Abspielgerät wird daher den ersten Teil der Multimediadaten ohne nennenswerte Verzögerung abspielen können. Damit ist bereits auf einfache und effiziente Art und Weise eine effektive Preview- bzw. Prelisten-Funktion möglich.

Das Bereitstellen eines unverschlüsselten Anfangsabschnitts des Nutzdatenblocks bringt jedoch weitere erhebliche Vorteile mit sich, wenn die Entschlüsselungsvorrichtungen über begrenzte Speicher- und Prozessorressourcen verfügen, was insbesondere bei Solid-State-Playern der Fall ist, die möglichst preiswert auf dem Markt angeboten werden müssen. Wenn zu verschlüsselnde Multimediadaten beispielsweise durch irgendein MPEG-Verfahren codiert sind, so muß ein Abspielgerät, um den Anfangsabschnitt des Nutzdatenblocks abspielen zu können, die Multimediadaten lediglich decodieren und dann abspielen. Das Abspielgerät hat daher während des Decodierens und Abspielens noch freie Prozessorressourcen, um während des Abspielens des Anfangsabschnitts des Nutzdatenblocks, der unverschlüsselt ist, den Anfangsblock selbst vollständig zu verarbeiten, um den dann folgenden verschlüsselten Teil des Nutzdatenblocks zu entschlüsseln, zu decodieren und abzuspielen.

Die erfindungsgemäße Bereitstellung eines unverschlüsselten Anfangsabschnitts des Nutzdatenblocks ermöglicht daher eine Verteilung von benötigten Speicher- und Prozessorressourcen, derart, daß auch mit Abspielgeräten mit begrenzten Ressourcen ein Entschlüsseln, Decodieren und Abspielen von Multimediadaten ohne außerordentlich hohe Verzögerung erreicht wird.

Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend bezugnehmend auf die beiliegenden Zeichnungen detailliert erläutert. Es zeigen:

Fig. 1 einen Multimediadaten-Strom, der gemäß der vorliegenden Erfindung erzeugt werden kann;

Fig. 2 eine detailliertere Darstellung des Anfangsblocks und des Nutzdatenblocks des verschlüsselten Multimediadatenstroms;

Fig. 3 eine Auswahl bestimmter Einträge in die einzelnen Unterblöcke des Anfangsblocks;

Fig. 4 ein Flußdiagramm des erfindungsgemäßen Verfahrens zum Erzeugen eines verschlüsselten Multimediadatenstroms; und

Fig. 5 ein Flußdiagramm des erfindungsgemäßen Verfahrens zum Abspielen eines verschlüsselten Multimediadatenstroms.

Fig. 1 zeigt einen verschlüsselten Multimediadatenstrom 10, der einen Anfangsblock oder Header 12 und einen Nutzdatenblock 14, d. h. einen Block mit verschlüsselten Multimediadaten, aufweist. Der Nutzdatenblock 14 umfaßt verschlüsselte Abschnitte 16 und unverschlüsselte Abschnitte 18 zwischen den verschlüsselten Abschnitten 16. Außerdem umfaßt ein Multimediadatenstrom, der gemäß der vorliegenden Erfindung erzeugt werden kann, einen weiteren unverschlüsselten Abschnitt 20, der auf den Anfangsblock 12 folgt und vor einem verschlüsselten Abschnitt 16 angeordnet ist.

Üblicherweise sind die zu verschlüsselten Multimediadaten auf irgendeine Art und Weise codiert, wie z. B. nach einem MPEG-Standard, wie z. B. MPEG-2 AAC, MPEG-4 AAC oder MPEG Layer-3. Daher ist es ausreichend, gewisse Abschnitte der zu verschlüsselten Multimediadaten zu verschlüsseln. Dies führt

zu einem wesentlich verringerten Verarbeitungsaufwand sowohl beim Provider, der die Daten verschlüsselt, als auch beim Kunden, der die Daten wieder entschlüsseln muß. Außerdem wird durch die lediglich teilweise Verschlüsselung der Multimediadaten der Hörgenuß bzw. der Sehgenuß eines Benutzers, der lediglich die unverschlüsselten Multimediadaten verwendet, durch die ständig auftretenden verschlüsselten Blöcke stark beeinträchtigt.

Obwohl Fig. 1 einen verschlüsselten Multimediadatenstrom zeigt, bei dem der Anfangsblock 12 am Anfang des verschlüsselten Multimediadatenstroms angeordnet ist, soll sich diese Anordnung von Anfangsblock und Nutzdatenblock nicht auf die Übertragung des verschlüsselten Multimediadatenstroms beziehen. Der Ausdruck "Anfangsblock" soll lediglich zum Ausdruck bringen, daß eine Entschlüsselungsvorrichtung, die den verschlüsselten Multimediadatenstrom entschlüsseln möchte, zunächst zumindest Teile des Anfangsblocks benötigt, bevor die Multimediadaten selbst entschlüsselt werden können. Je nach Übertragungsmedium könnte der Anfangsblock irgendwo auch innerhalb des Nutzdatenblocks angeordnet sein bzw. durchaus nach bestimmten Teilen des Nutzdatenblocks empfangen werden, wenn beispielsweise an eine Paket-orientierte Übertragung des Multimediadatenstroms gedacht wird, bei der unterschiedliche Pakete, von denen eines den Anfangsblock enthalten kann und ein anderes einen Teil des Nutzdatenblocks enthalten kann, über unterschiedliche physische Übertragungswege übertragen werden, derart, daß die Empfangsreihenfolge ganz und gar nicht der Sendereihenfolge entsprechen muß. Eine Entschlüsselungsvorrichtung muß in diesem Fall jedoch in der Lage sein, die empfangenen Pakete zu speichern und wieder zu ordnen, derart, daß Informationen aus dem Anfangsblock extrahiert werden, um mit dem Entschlüsseln zu beginnen. Der verschlüsselte Multimediadatenstrom könnte ferner in Form einer Datei vorliegen oder aber auch in Form eines tatsächlichen Datenstroms, wenn beispielsweise an eine Live-Übertragung eines Multimediaereignisses gedacht wird. Diese Anwendung wird insbesondere beim digitalen Benutzer-selektiven

Rundfunk auftreten.

Die Länge eines verschlüsselten Abschnitts 16 wird durch einen Wert Menge 22 dargestellt, während der Abstand im verschlüsselten Multimediadatenstrom von dem Beginn eines verschlüsselten Abschnitts 16 bis zum Beginn des nächsten verschlüsselten Abschnitts 16 mit Schritt 24 bezeichnet wird. Die Länge des weiteren verschlüsselten Abschnitts 20 wird durch einen Wert Erster Schritt 26 angegeben.

Diese Werte 22, 24 und 26 werden selbstverständlich für ein korrektes Entschlüsseln der Multimediadaten in einer Entschlüsselungsvorrichtung benötigt, weshalb dieselben in den Anfangsblock 12 eingetragen werden müssen, wie es später erläutert wird.

Es ist jedoch zu bemerken, daß das Größenverhältnis der Werte 22 und 24 variabel sein kann. Dieses schließt auch ein, daß der unverschlüsselte Bereich 18 die Länge Null aufweist, daß also eine vollständige Verschlüsselung vorgenommen wird

Fig. 2 zeigt eine detailliertere Darstellung des verschlüsselten Multimediadatenstroms 10, der aus dem Anfangsblock 12 und dem Nutzdatenblock 14 besteht. Der Anfangsblock 12 ist in mehrere Unterblöcke unterteilt, die im einzelnen insbesondere bezugnehmend auf Fig. 3 erläutert werden. Es sei darauf hingewiesen, daß die Anzahl und Funktion der Unterblöcke beliebig erweitert werden kann. In Fig. 2 sind daher lediglich beispielhaft einzelne Unterblöcke des Anfangsblocks 12 aufgeführt. Derselbe umfaßt, wie es in Fig. 2 gezeigt ist, einen sogenannten Crypt-Block 29, der allgemein gesagt für das Verschlüsseln der Multimediadaten relevante Informationen aufweist. Weiterhin umfaßt der Anfangsblock 12 einen sogenannten Lizenz-Block 30, der Daten aufweist, die sich auf die Art und Weise beziehen, wie ein Benutzer den verschlüsselten Multimediadatenstrom verwenden kann bzw. darf. Der Anfangsblock 12 umfaßt ferner einen Nutzdatenin-

fo-Block 32, der Informationen bezüglich des Nutzdatenblocks 14 sowie generelle Informationen über den Anfangsblock 12 selbst umfassen kann. Weiterhin kann der Anfangsblock 12 einen Alter-Anfangsblock-Block 34 aufweisen, der eine sogenannte rekursive Anfangsblock-Struktur ermöglicht. Dieser Block versetzt den Benutzer, der neben einer Entschlüsselungsvorrichtung auch eine Verschlüsselungsvorrichtung hat, in die Lage, einen verschlüsselten Multimediadatenstrom für andere in seinem Besitz befindliche Abspielgeräte umzuformatieren, ohne die ursprünglichen vom Distributor gelieferten Anfangsblockinformationen zu verlieren bzw. zu modifizieren. Je nach Anwendungsbereich können noch weitere Unterblöcke, wie z. B. ein IP-Information-Block (IP = Intellectual Property = Geistiges Eigentum) nach ISO/IEC 14496-1, MPEG-4, Systems, 1998, der Urheberrechtsinformationen umfaßt, zu dem Anfangsblock 12 hinzugefügt werden.

Wie es in der Technik üblich ist, kann jedem Block eine interne Blockstruktur zugewiesen werden, die zunächst einen Blockidentifikator fordert, die dann die Länge des Unterblocks umfaßt, und die dann schließlich die Block-Nutzdaten selbst aufführt. Damit erhält der verschlüsselte Multimediadatenstrom und insbesondere der Anfangsblock des verschlüsselten Multimediadatenstroms einer erhöhte Flexibilität, derart, daß auf neue Anforderungen insoweit reagiert werden kann, daß zusätzliche Unterblöcke hinzugefügt werden bzw. bestehende Unterblöcke weggelassen werden können.

Fig. 3 gibt eine Übersicht über die Block-Nutzdaten der einzelnen in Fig. 2 dargestellten Unterblöcke.

Zunächst wird auf den Crypt-Block 28 eingegangen. Derselbe enthält einen Eintrag für einen Multimediadaten-Verschlüsselungsalgorithmus 40, der den bei einem bevorzugten Ausführungsbeispiel verwendeten symmetrischen Verschlüsselungsalgorithmus identifiziert, der beim Verschlüsseln der Multimediadaten verwendet worden ist. Der Eintrag 40 dürfte ein Index für eine Tabelle sein, derart, daß eine Entschlüsse-

lungsvorrichtung nach Lesen des Eintrags 40 in der Lage ist, denselben Verschlüsselungsalgorithmus aus einer Vielzahl von Verschlüsselungsalgorithmen auszuwählen, den die Verschlüsselungsvorrichtung verwendet hat. Der Crypt-Block 28 umfaßt ferner den Eintrag Erster Schritt 26, den Eintrag Schritt 24 und den Eintrag Menge 22, die bereits in Verbindung mit Fig. 1 dargestellt worden sind. Diese Einträge in dem Anfangsblock versetzen eine Entschlüsselungsvorrichtung in die Lage, einen verschlüsselten Multimediadatenstrom entsprechend unterzugliedern, um eine korrekte Entschlüsselung durchführen zu können.

Der Crypt-Block 28 enthält ferner einen Eintrag für den Distributor bzw. Provider bzw. Lieferanten 42, der ein Code für den Distributor ist, der den verschlüsselten Multimediadatenstrom erzeugt hat. Ein Eintrag Benutzer 44 identifiziert den Benutzer, der von dem Distributor, der durch den Eintrag 42 identifiziert ist, den verschlüsselten Multimediadatenstrom auf irgendeine Art und Weise erhalten hat. Eine mögliche Verwendung dieser Kennungen ist es, die Benutzerkennung gerätespezifisch durchzuführen. Der Eintrag Benutzer würde dann die Seriennummer eines PC, eines Laptops, eines Auto-HiFi-Geräts, einer Heim-Stereoanlage etc. umfassen, die ein Abspielen nur auf dem speziellen Gerät zuläßt. Zur weiteren Erhöhung der Flexibilität und/oder Sicherheit könnte statt der Seriennummer, die bei jedem Hersteller unterschiedlich aussieht, die aber zufällig identisch sein könnten, eine spezielle Kennung, wie z. B. eine logische Verknüpfung der Festplattengröße mit der Prozessornummer etc. beim Beispiel eines PC, eingesetzt werden.

Ein Eintrag 46 enthält einen Ausgabewert, auf den später detailliert eingegangen wird. Dieser Ausgabewert stellt allgemein gesagt eine verschlüsselte Version des Multimediadaten-Schlüssels dar, der in Verbindung mit dem durch den Eintrag 40 identifizierten Multimediadaten-Verschlüsselungsalgorithmus benötigt wird, um die in dem Nutzdatenblock 14

vorhandenen verschlüsselten Multimediadaten (Abschnitte 16 von Fig. 1) korrekt zu entschlüsseln. Um eine ausreichende Flexibilität für zukünftige Anwendungen zu haben, sind ferner die beiden Einträge Ausgabewertlänge 48 und Ausgabewertmaske 50 vorgesehen. Der Eintrag Ausgabewertlänge 48 gibt an, welche Länge der Ausgabewert 46 tatsächlich hat. Um ein flexibles Anfangsblockformat zu erhalten, sind jedoch in dem Anfangsblockformat für den Ausgabewert mehr Byte vorgesehen als ein Ausgabewert derzeit tatsächlich hat. Die Ausgabewertmaske 50 gibt daher an, wie ein kürzerer Ausgabewert auf einen längeren Ausgabewertplatz gewissermaßen verteilt wird. Ist die Ausgabewertlänge beispielsweise halb so groß wie der verfügbare Platz für den Ausgabewert, so könnte die Ausgabewertmaske derart gestaltet sein, daß die erste Hälfte der Ausgabewertmaske gesetzt ist, während die zweite Hälfte abgedeckt ist. Dann würde der Ausgabewert einfach in den von der Syntax für den Anfangsblock vorgesehenen Raum eingetragen werden und die erste Hälfte einnehmen, während die andere Hälfte aufgrund der Ausgabewertmaske 50 ignoriert wird.

Im nachfolgenden wird auf den Lizenz-Block 30 des Anfangsblocks 12 eingegangen. Derselbe umfaßt einen Eintrag Bitmaske 52. Dieser Eintrag kann bestimmte spezielle Informationen für das Abspielen bzw. für die generelle Art der Verwendung der verschlüsselten Multimediadaten haben. Insbesondere könnte hiermit einer Entschlüsselungsvorrichtung mitgeteilt werden, ob bzw. ob nicht die Nutzdaten lokal abgespielt werden können. Weiterhin könnte hier signalisiert werden, ob das Herausforderungs-Antwort-Verfahren zum Verschlüsseln eingesetzt worden ist, das in dem eingangs erwähnten Deutschen Patent DE 196 25 635 C1 beschrieben ist und einen effizienten Datenbankzugriff ermöglicht.

Ein Eintrag Verfallsdatum 54 gibt den Zeitpunkt an, zu dem die Erlaubnis, den verschlüsselten Multimediadatenstrom zu entschlüsseln, erlischt. Eine Entschlüsselungsvorrichtung wird in diesem Fall den Eintrag Verfallsdatum 54 prüfen und

mit einer eingebauten Zeitmeßeinrichtung vergleichen, um im Falle, daß das Verfallsdatum bereits überschritten ist, keine Entschlüsselung des verschlüsselten Multimediadatenstroms mehr durchzuführen. Dies erlaubt es einem Provider, auch zeitlich begrenzt verschlüsselte Multimediadaten zur Verfügung zu stellen, was den Vorteil einer wesentlich flexibleren Handhabung und auch Preisgestaltung ermöglicht. Diese Flexibilität wird weiter durch einen Eintrag Anfangsdatum 56 unterstützt, in dem spezifiziert ist, ab wann eine verschlüsselte Multimediadatei entschlüsselt werden darf. Eine Verschlüsselungsvorrichtung wird den Eintrag Anfangsdatum mit ihrer eingebauten Uhr vergleichen, um erst dann eine Entschlüsselung der verschlüsselten Multimediadaten durchzuführen, wenn der aktuelle Zeitpunkt später als das Anfangsdatum 56 ist.

Ein Eintrag Erlaubte Abspielanzahl 58 gibt an, wie oft der verschlüsselte Multimediadatenstrom entschlüsselt, d. h. abgespielt werden darf. Dies erhöht weiter die Flexibilität des Providers, derart, daß er nur eine bestimmte Anzahl des Abspielens beispielsweise gegen eine bestimmte Summe zuläßt, die kleiner ist als eine Summe, die für die unbeschränkte Nutzung des verschlüsselten Multimediadatenstroms anfallen würde.

Zur Verifizierung bzw. Unterstützung des Eintrags Erlaubte Abspielanzahl 58 umfaßt der Lizenz-Block 30 ferner einen Eintrag Tatsächliche Abspielanzahl 60, der nach jedem Entschlüsseln des verschlüsselten Multimediadatenstroms beispielsweise um Eins inkrementiert werden könnte. Eine Entschlüsselungsvorrichtung wird daher immer überprüfen, ob der Eintrag Tatsächliche Abspielanzahl kleiner als der Eintrag Erlaubte Abspielanzahl ist. Wenn dies der Fall ist, wird eine Entschlüsselung der Multimediadaten durchgeführt. Wenn dies nicht der Fall ist, wird keine Entschlüsselung mehr ausgeführt.

Analog zu den Einträgen 58 und 60 sind die Einträge Erlaubte

Kopieanzahl 62 und Tatsächliche Kopieanzahl 64 implementiert. Durch die beiden Einträge 62 und 64 wird sichergestellt, daß ein Benutzer der Multimediadaten dieselben lediglich so oft kopiert, wie es ihm vom Provider erlaubt wird, bzw. so oft, wie er beim Kauf der Multimediadaten bezahlt hat. Durch die Einträge 58 bis 64 wird ein effektiver Urheberrechtsschutz sichergestellt, und kann eine Selektion zwischen privaten Nutzern und gewerblichen Nutzern erreicht werden, beispielsweise, indem die Einträge Erlaubte Abspielanzahl 58 und Erlaubte Kopieanzahl 62 auf einen kleinen Wert eingestellt werden.

Die Lizenzierung könnte z. B. so gestaltet sein, daß eine bestimmte Anzahl von Kopien (Eintrag 62) des Originals erlaubt ist, während keine Kopien einer Kopie zulässig sind. Der Anfangsblock einer Kopie würde dann im Gegensatz zum Anfangsblock des Originals als Eintrag Erlaubte Kopieanzahl eine Null haben, derart, daß diese Kopie von einer ordnungsgemäßen Ver/Entschlüsselungsvorrichtung nicht mehr kopiert wird.

Bei dem hier gezeigten Beispiel für ein Multimediadatenschutzprotokoll (MMP; MMP = Multimedia Protection Protcol) enthält der Anfangsblock 12 ferner einen Nutzdaten-Informationsblock 32, der hier lediglich zwei Block-Nutzdateneinträge 66 und 68 hat, wobei der Eintrag 66 eine Hash-Summe über den gesamten Anfangsblock enthält, während der Eintrag 68 den Typ des Hash-Algorithmus identifiziert, der zum Bilden der Hash-Summe über den gesamten Anfangsblock verwendet worden ist.

In diesem Zusammenhang sei beispielsweise auf das Fachbuch "Applied Cryptography", Second Edition, John Wiley & Sons, Inc. von Bruce Schneier (ISBN 0 471-11709-9) verwiesen, das eine ausführliche Darstellung symmetrischer Verschlüsselungsalgorithmen, asymmetrischer Verschlüsselungsalgorithmen und Hash-Algorithmen umfaßt.

Der Anfangsblock 12 umfaßt schließlich den Alter-Anfangsblock-Block 34, der neben den Synchronisationsinformationen, die in Fig. 3 nicht dargestellt sind, den Eintrag Alter Anfangsblock 70 aufweist. In den Eintrag Alter-Anfangsblock 70 kann, wenn ein Benutzer selbst eine Verschlüsselung durchführt und somit einen neuen Anfangsblock 12 erzeugt, der alte Anfangsblock vom Provider bewahrt werden, um keine wesentlichen Informationen zu verlieren, die der Provider in den Anfangsblock eingetragen hat. Dazu könnten beispielsweise Urheberinformationen (IP-Information-Block) frühere Benutzerinformationen und Distributoreninformationen zählen, die eine Zurückverfolgung einer Multimediadatei, die beispielsweise mehrmals von unterschiedlichen Geräten ent-/ver-schlüsselt worden ist, auf den ursprünglichen Anbieter transparent ermöglichen, wobei Urheberinformationen bewahrt werden. Damit ist es möglich, jederzeit zu überprüfen, ob eine verschlüsselte Multimediadatei legal oder illegal erworben worden ist.

Es ist offensichtlich, daß die Reihenfolge der in Fig. 5 genannten Schritte ebenso variiert werden kann, wie es auch bezugnehmend auf Fig. 4 erläutert worden ist.

Fig. 4 zeigt ein Flußdiagramm des erfindungsgemäßen Verfahrens zum Erzeugen eines verschlüsselten Multimediadatenstroms. In einem Schritt 100 wird der Anfangsblock 12 erzeugt. Daran anschließend wird in einem Schritt 102 der erste Teil der zu verschlüsselnden Multimediadaten als Anfangsabschnitt des Nutzdatenblocks 14 verwendet, jedoch ohne diesen ersten Teil zu verschlüsseln. Der Anfangsabschnitt bildet daher den weiteren unverschlüsselten Abschnitt 20 von Fig. 1, dessen Länge durch den Eintrag Erster Schritt 26 in dem Anfangsblock spezifiziert ist. Daran anschließend wird der zweite Teil der zu verschlüsselnden Multimediadaten in einem Schritt 104 verschlüsselt, um den auf den weiteren unverschlüsselten Abschnitt 20 folgenden verschlüsselten Abschnitt 16 (Fig. 1) zu erzeugen. Um einen einfachen verschlüsselten Multimediadatenstrom fertigzustellen, wird der

verschlüsselte zweite Teil an den Anfangsabschnitt des Nutzdatenblocks angehängt (Schritt 106), derart, daß der verschlüsselte Multimediadatenstrom 10 den Anfangsblock 12, den Anfangsabschnitt 20 und den verschlüsselten zweiten Teil 16 aufweist. Der verschlüsselte Multimediadatenstrom kann nun beliebig fortgesetzt werden, indem wieder ein unverschlüsselter Abschnitt 18, ein verschlüsselter Abschnitt 16 etc. generiert und in den Nutzdatenblock 14 geschrieben wird.

Aus Fig. 4 ist ersichtlich, daß die Reihenfolge der Schritte 100 bis 106 nicht zwingend festgelegt ist. Der Anfangsblock könnte auch erst nach der Fertigstellung des Nutzdatenblocks erzeugt werden und mittels eines Blockmultiplexers an den Beginn des Nutzdatenblocks gestellt werden. Alternativ könnte der zweite Teil der zu verschlüsselnden Multimediadaten verschlüsselt werden (Schritt 104), bevor der erste Teil in den Datenblock geschrieben worden ist. Der Eintrag Erster Schritt 26 definiert nämlich genau den Punkt, d. h. die Bitstelle, des Nutzdatenblocks 14, an dem mit dem Eintragen des verschlüsselten zweiten Teils begonnen werden muß. Wesentlich ist daher lediglich, daß der unverschlüsselte Anfangsabschnitt 20 des Nutzdatenblocks 14 unmittelbar hinter den Anfangsblock 12 gestellt wird. An dieser Stelle sei noch einmal darauf hingewiesen, daß die hier beschriebene Reihenfolge Anfangsblock, unverschlüsselter Anfangsabschnitt und verschlüsselter zweiter Teil (d. h. 12, 20, 16) lediglich die Reihenfolge beschreibt, in der der Multimediadatenstrom im Abspielgerät angeordnet werden muß, damit sich die erfindungsgemäßen Vorteile ergeben. Diese Reihenfolge hat keine Auswirkung auf die Übertragung des verschlüsselten Multimediadatenstroms. Dies wird besonders dort offensichtlich, wo eine paketorientierte Datenübertragung eingesetzt wird. Ein Paket für den Anfangsblock, ein Paket für den Anfangsabschnitt und ein Paket für den verschlüsselten zweiten Teil könnten über unterschiedliche Wege von einem Sender zu einem Empfänger übermittelt werden, derart, daß zuerst der Anfangsabschnitt und dann der verschlüsselte zweite Teil und schließlich der Anfangsblock eintreffen. Das Abspielgerät

muß in diesem Fall jedoch in der Lage sein, die drei Pakete wieder entsprechend anzuordnen, wie es beschrieben worden ist.

Fig. 5 zeigt ein Flußdiagramm des erfindungsgemäßen Verfahrens zum Abspielen des verschlüsselten Multimediadatenstroms 10, der den Anfangsblock 12, den unverschlüsselten Anfangsabschnitt 20 des Nutzdatenblocks 14 und den verschlüsselten zweiten Teil 16 des Nutzdatenblocks 14 aufweist. Erfindungsgemäß werden im Abspielgerät zunächst lediglich die Informationen des Anfangsblocks 12 verarbeitet, die zum Abspielen des unverschlüsselten Anfangsabschnitts des Nutzdatenblocks 14 unbedingt erforderlich sind (Schritt 110).

Anschließend kann bereits mit minimaler Verzögerung der unverschlüsselte Anfangsabschnitt 20 des Nutzdatenblocks 14 abgespielt werden (Schritt 112). Damit ist eine einfache und effiziente Preview- bzw. Prelisten-Funktion implementiert. Üblicherweise wird das Abspielen des Anfangsabschnitts des Nutzdatenblocks (Schritt 112) nicht die volle Prozessorleistung des Abspielgeräts in Anspruch nehmen. Das Abspielgerät kann daher im wesentlichen parallel zum Abspielen des Anfangsabschnitts die anderen Informationen des Anfangsblocks 12 verarbeiten, d. h. die Informationen, die zum Abspielen des Anfangsabschnitts des Nutzdatenblocks nicht benötigt werden (Schritt 114). Das Abspielgerät wird dann, wenn der Anfangsblock 12 verarbeitet ist, die verschlüsselten Multimediadaten im ersten verschlüsselten Abschnitt 16, d. h. dem verschlüsselten zweiten Teil des Nutzdatenblocks 14, entschlüsseln können (Schritt 116), um schließlich die entschlüsselten Multimediadaten des zweiten Abschnitts abspielen zu können (Schritt 118).

Bezugnehmend auf Fig. 3 wird im nachfolgenden auf die Informationen eingegangen, die zum Abspielen des unverschlüsselten Anfangsabschnitts 20 unbedingt erforderlich sind. Unbedingt erforderliche Informationen sind zum einen die in Fig. 3 nicht dargestellten allgemeinen Blockidentifikati-

onsinformationen und Blocklängeninformationen, damit ein Abspielgerät die richtige Stelle des Anfangsblocks ermittelt, wo nötige Informationen stehen. Sind die Multimediadaten, wie es üblicherweise der Fall ist, auf irgendeine Art und Weise beispielsweise nach einem MPEG-Verfahren codiert, so wird das Abspielgerät im Schritt 110 (Fig. 5) diese Informationen aus dem Anfangsblock 12 extrahieren müssen. In der Tabelle in Fig. 3 stehen diese Informationen im Eintrag Nutzdaten-Typ des Nutzdaten-Blocks 14. Nun weiß das Abspielgerät, daß die unverschlüsselten Daten im Anfangsabschnitt 20 des Nutzdatenblocks 14 beispielsweise im MPEG-Layer-3-Format (MP3) vorliegen, derart, daß das Abspielgerät die unverschlüsselten Multimediadaten decodieren und abspielen kann (Schritt 112). Während des Abspielens des Anfangsabschnitts 20 ist das Gerät nun in der Lage, sämtliche relativ komplizierten weiteren Daten des Anfangsabschnitts zu verarbeiten, wie z. B. die Daten im Crypt-Block 28, im Lizenz-Block 30, im Nutzdaten-Informations-Block 32, der insbesondere eine relativ aufwendige Hash-Summe/digitale Unterschrift über den Anfangsblock (Eintrag 66) umfaßt. Eine weitere aufwendige Operation besteht in der Entschlüsselung des Multimediadaten-Schlüssels aus dem Ausgabewert (Eintrag 46), um die verschlüsselten Abschnitte 16 (Fig. 1) des verschlüsselten Multimediadatenstroms entschlüsseln zu können.

Es kann wahlweise eingestellt werden, ob zu den Informationen, die zum Abspielen des unverschlüsselten Anfangsabschnitts 20 nötig sind, auch die Einträge Lieferant (Distributor) 42 und Benutzer 44 gehören sollen. In diesem Fall ist die Preview- bzw. Prelisten-Funktion lediglich für einen bestimmten Benutzer bzw. für Abonnenten eines bestimmten Distributors möglich. Somit kann ein Distributor durch die sehr einfache und nicht-aufwendige Implementation der Preview- bzw. Prelisten-Funktion einem speziellen Benutzer bzw. allen seinen abonnierten Benutzern eine verschlüsselte Multimediadatei schicken, damit der/die Benutzer "auf den Geschmack" kommt/kommen, indem er einen Bereich von z. B. 1

Sekunde bis zu 1 Minute, d. h. den unverschlüsselten Anfangsabschnitt 20 anhört bzw. ansieht, um sich dann zum Kauf des gesamten verschlüsselten Multimediadatenstroms zu entscheiden, bzw. um einzelne Stücke auf einfache Art und Weise identifizieren zu können.

In diesem Fall brauchen die Schritte 114, 116 und 118 nicht ausgeführt zu werden. Es sei darauf hingewiesen, daß dieselben in diesem Fall auch gar nicht ausgeführt werden können, da der Benutzer unter Umständen noch nicht im Besitz der Informationen ist, wie der Ausgabewert 46 entschlüsselt werden muß, um den Multimediadaten-Schlüssel zu erhalten, um die verschlüsselten Multimediadaten in den verschlüsselten Abschnitten 16 entschlüsseln zu können. Sollte sich ein Benutzer zum Kauf entschließen, nachdem er durch die Preview- bzw. Prelisten-Funktion auf den Geschmack gekommen ist, so muß der Distributor lediglich den Benutzer in die Lage versetzen, den Ausgabewert zu entschlüsseln.

Das Bereitstellen eines unverschlüsselten Anfangsabschnitts im Nutzdatenblock ermöglicht daher einerseits die einfache Preview- bzw. Prelisten-Funktion und andererseits die Verwendung von Prozessoren mit begrenzten Speicher- bzw. Prozessorressourcen, ohne daß wesentliche Verzögerungen durch die Verarbeitung des gesamten Anfangsblocks in Kauf genommen werden müssen.

Patentansprüche

1. Verfahren zum Erzeugen eines verschlüsselten Nutzdatenstroms (10), der einen Anfangsblock (12) und einen Nutzdatenblock (14) aufweist, mit folgenden Schritten:

   Erzeugen (100) des Anfangsblocks (12); und

   Erzeugen (102, 104, 106) des Nutzdatenblocks (14) durch folgende Teilschritte:

      Verwenden (102) eines ersten Teils der zu verschlüsselnden Nutzdaten als Anfangsabschnitt (20) für den Nutzdatenblock (14), wobei der Anfangsabschnitt (20) unverschlüsselt ist;

      Verschlüsseln (104) eines zweiten Teils von zu verschlüsselnden Nutzdaten, die auf den ersten Teil folgen; und

      Anhängen (106) der verschlüsselten Nutzdaten (16) an den unverschlüsselten Anfangsabschnitt (20).

2. Verfahren nach Anspruch 1, bei dem der Schritt des Erzeugens (100) des Anfangsblocks (12) folgenden Teilschritt aufweist:

   Eintragen der Länge (26) des Anfangsabschnitts (20) in den Anfangsblock (12).

3. Verfahren nach Anspruch 1 oder 2, bei dem der zweite Teil nicht sämtliche zu verschlüsselnde Nutzdaten umfaßt, und bei dem der Schritt des Erzeugens (102, 104, 106) des Nutzdatenblocks folgenden Teilschritt aufweist:

   Anhängen eines dritten Teils (18) von zu verschlüs-

selnden Nutzdaten, die auf den zweiten Teil folgen, an die verschlüsselten Nutzdaten (16) des zweiten Teils, wobei die Nutzdaten des dritten Teils unverschlüsselt sind.

4. Verfahren nach einem der vorhergehenden Ansprüche, bei dem der Schritt des Erzeugens (100) des Anfangsblocks (12) folgenden Teilschritt aufweist:

Eintragen der Länge (22) der verschlüsselten Multimediadaten (16), die den zu verschlüsselnden Nutzdaten des zweiten Teils entsprechen, in den Anfangsblock (12).

5. Verfahren nach Anspruch 3 oder 4, bei dem der Schritt des Erzeugens (100) des Anfangsblocks (12) ferner folgenden Teilschritt aufweist:

Eintragen der Summe (24) der Länge (22) der verschlüsselten Nutzdaten, die dem zweiten Teil entsprechen, und der Länge des dritten Teils der unverschlüsselten Nutzdaten (18) in den Anfangsblock (12).

6. Verfahren zum Abspielen eines verschlüsselten Multimediadatenstroms (10), der einen Anfangsblock (12) und einen Nutzdatenblock (14) aufweist, wobei ein Anfangsabschnitt (20) des Nutzdatenblocks (14), der auf den Anfangsblock (12) folgt, unverschlüsselte Nutzdaten aufweist, und wobei ein weiterer Abschnitt (16) des Nutzdatenblocks (14) verschlüsselte Nutzdaten aufweist, wobei der Anfangsblock (12) Informationen enthält, die zum Abspielen des Anfangsabschnitts (20) des Nutzdatenblocks (14) benötigt werden, und wobei der Anfangsblock (12) Informationen enthält, die zum Abspielen des unverschlüsselten Anfangsabschnitts (20) des Nutzdatenblocks (14) nicht benötigt werden, mit folgenden Schritten:

Verarbeiten (110) der Informationen des Anfangsblocks (12), die zum Abspielen des Anfangsabschnitts (20) des Nutzdatenblocks (14) benötigt werden; und

Abspielen (112) des unverschlüsselten Anfangsabschnitts (20) des Nutzdatenblocks (14).

7. Verfahren nach Anspruch 6, das ferner folgende Schritte aufweist:

Verarbeiten (114) der Informationen des Anfangsblocks (12), die zum Abspielen des unverschlüsselten Anfangsabschnitts (20) nicht benötigt werden;

Entschlüsseln des weiteren Abschnitts (16) des Nutzdatenblocks (14) unter Verwendung der verarbeiteten Informationen des Anfangsblocks (12); und

Abspielen (118) der entschlüsselten Nutzdaten des weiteren Abschnitts (16) des Nutzdatenblocks (14).

8. Verfahren nach Anspruch 7, bei dem der Schritt des Verarbeitens (114) der Informationen des Anfangsblocks (12), die zum Abspielen des unverschlüsselten Anfangsabschnitts (20) nicht benötigt werden, im wesentlichen parallel zum Abspielen (112) des unverschlüsselten Anfangsabschnitts (20) durchgeführt werden.

9. Verfahren nach einem der Ansprüche 6 bis 8, bei dem die Länge (22) des unverschlüsselten Anfangsabschnitts (20) des Nutzdatenblocks (14) zwischen 1 und 60 Sekunden liegt.

10. Verfahren nach einem der Ansprüche 6 bis 9, bei dem die zu verschlüsselnden Nutzdaten codiert sind, und bei dem die Informationen, die zum Abspielen benötigt werden, einen Eintrag (72) bezüglich des Typs des Codier/Decodier-Verfahrens aufweisen.

11. Verfahren nach einem der vorhergehenden Ansprüche, bei dem die Nutzdaten Audio- und/oder Videodaten sind.

12. Vorichtung zum Erzeugen eines verschlüsselten Nutzdatenstroms (10), der einen Anfangsblock (12) und einen Nutzdatenblock (14) aufweist, mit folgenden Merkmalen:

einer Einrichtung zum Erzeugen (100) des Anfangsblocks (12); und

einer Einrichtung zum Erzeugen (102, 104, 106) des Nutzdatenblocks (14), die folgende Merkmale aufweist:

eine Einrichtung zum Verwenden (102) eines ersten Teils der zu verschlüsselnden Nutzdaten als Anfangsabschnitt (20) für den Nutzdatenblock (14), wobei der Anfangsabschnitt (20) unverschlüsselt ist;

eine Einrichtung zum Verschlüsseln (104) eines zweiten Teils von zu verschlüsselnden Nutzdaten, die auf den ersten Teil folgen; und

eine Einrichtung zum Anhängen (106) der verschlüsselten Nutzdaten (16) an den unverschlüsselten Anfangsabschnitt (20).

13. Vorrichtung zum Abspielen eines verschlüsselten Nutzdatenstroms (10), der einen Anfangsblock (12) und einen Nutzdatenblock (14) aufweist, wobei ein Anfangsabschnitt (20) des Nutzdatenblocks (14), der auf den Anfangsblock (12) folgt, unverschlüsselte Nutzdaten aufweist, und wobei ein weiterer Abschnitt (16) des Nutzdatenblocks (14) verschlüsselte Nutzdaten aufweist, wobei der Anfangsblock (12) Informationen enthält, die zum Abspielen des Anfangsabschnitts (20) des Nutzdatenblocks (14) benötigt werden, und wobei der Anfangsblock

(12) Informationen enthält, die zum Abspielen des unverschlüsselten Anfangsabschnitts (20) des Nutzdatenblocks (14) nicht benötigt werden, mit folgenden Merkmalen:

einer Einrichtung zum Verarbeiten (110) der Informationen des Anfangsblocks (12), die zum Abspielen des Anfangsabschnitts (20) des Nutzdatenblocks (14) benötigt werden; und

einer Einrichtung zum Abspielen (112) des unverschlüsselten Anfangsabschnitts (20) des Nutzdatenblocks (14).

14. Vorrichtung nach Anspruch 13, die ferner folgende Merkmale aufweist:

eine Einrichtung zum Verarbeiten (114) der Informationen des Anfangsblocks (12), die zum Abspielen des unverschlüsselten Anfangsabschnitts (20) nicht benötigt werden;

eine Einrichtung zum Entschlüsseln des weiteren Abschnitts (16) des Nutzdatenblocks (14) unter Verwendung der verarbeiteten Informationen des Anfangsblocks (12); und

eine Einrichtung zum Abspielen (118) der entschlüsselten Nutzdaten des weiteren Abschnitts (16) des Nutzdatenblocks (14).

15. Vorrichtung nach Anspruch 14, bei der die Einrichtung zum Verarbeiten (114) der Informationen des Anfangsblocks (12), die zum Abspielen des unverschlüsselten Anfangsabschnitts (20) nicht benötigt werden, angeordnet ist, um im wesentlichen parallel zur Einrichtung zum Abspielen (112) des unverschlüsselten Anfangsabschnitts (20) betrieben zu werden.

16. Vorrichtung nach Anspruch 13, die als Stereoanlage, Hi-fi-Gerät, Solid-State-Player, Abspielgerät mit Festplatte oder CD-ROM, oder Computer ausgeführt ist.

17. Vorrichtung nach einem der Ansprüche 12 bis 16, bei der die Nutzdaten Audio- und/oder Videodaten sind.

Verfahren und Vorrichtung zum Erzeugen eines verschlüsselten Nutzdatenstroms und Verfahren und Vorrichtung zum Abspielen eines verschlüsselten Nutzdatenstroms

Zusammenfassung

Bei einem Verfahren zum Erzeugen eines verschlüsselten Multimediadatenstroms wird zunächst ein Anfangsblock (12) und dann ein Nutzdatenblock (14) erzeugt. Der Anfangsabschnitt (20) des Nutzdatenblocks enthält unverschlüsselte Nutzdaten, denen dann verschlüsselte Nutzdaten (16) folgen. Somit wird auf einfache Art und Weise eine Preview- bzw. Prelisten-Funktion implementiert. Weiterhin kann ein Abspielgerät den unverschlüsselten Anfangsabschnitt (20) bereits abspielen, während der vollständige Anfangsblock verarbeitet wird, um einen Multimediadatenschlüssel zu erhalten, um Hash-Summen usw. zu erzeugen. Durch diese parallele Verarbeitung können Abspielgeräte mit begrenzten Speicher- und Prozessorressourcen eingesetzt werden, ohne überlange Verzögerungen in Kauf nehmen zu müssen.

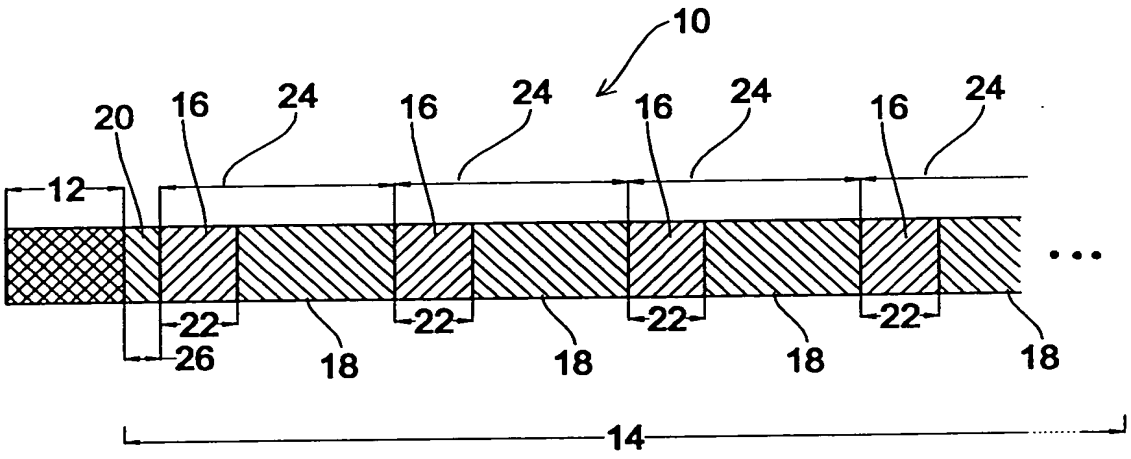
10
20
16
24
16
24
16
24
16
24
12
22
26
18
22
18
22
18
22
18
14

Fig. 1

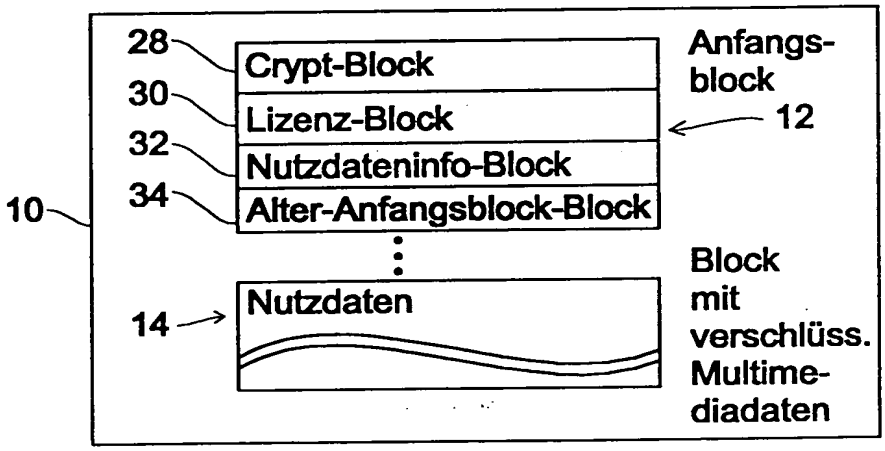
28
Crypt-Block
30
Lizenz-Block
32
Nutzdateninfo-Block
34
Alter-Anfangsblock-Block
Anfangs-
block
12
10
14
Nutzdaten
Block
mit
verschlüss.
Multime-
diadaten

Fig. 2

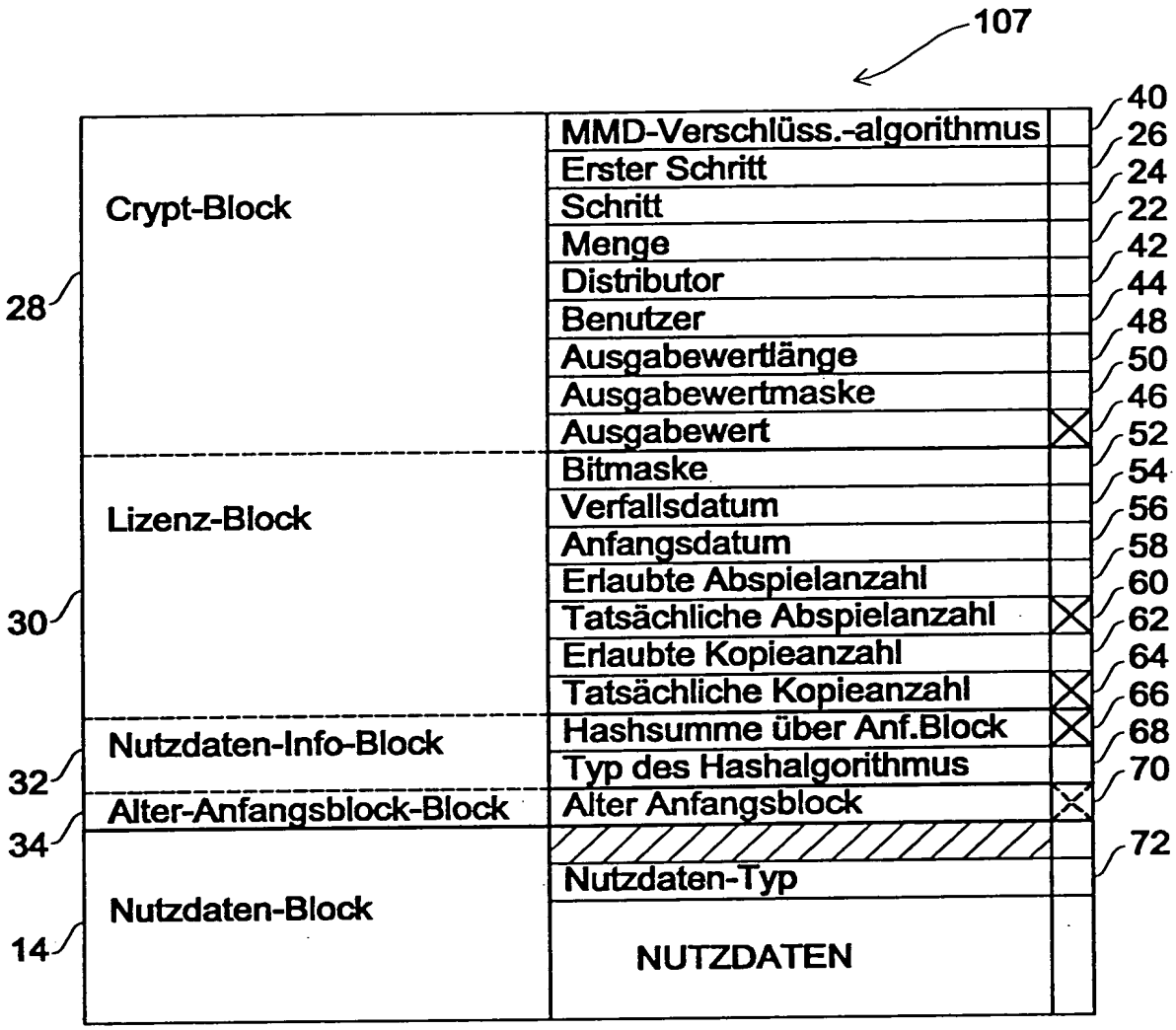
107
Crypt-Block
28
MMD-Verschlüss.-algorithmus
Erster Schritt
Schritt
Menge
Distributor
Benutzer
Ausgabewertlänge
Ausgabewertmaske
Ausgabewert
40
26
24
22
42
44
48
50
46
52
Lizenz-Block
30
Bitmaske
Verfallsdatum
Anfangsdatum
Erlaubte Abspielanzahl
Tatsächliche Abspielanzahl
Erlaubte Kopieanzahl
Tatsächliche Kopieanzahl
54
56
58
60
62
64
66
Nutzdaten-Info-Block
32
Hashsumme über Anf.Block
Typ des Hashalgorithmus
68
70
Alter-Anfangsblock-Block
34
Alter Anfangsblock
72
Nutzdaten-Block
14
Nutzdaten-Typ
NUTZDATEN

Fig. 3

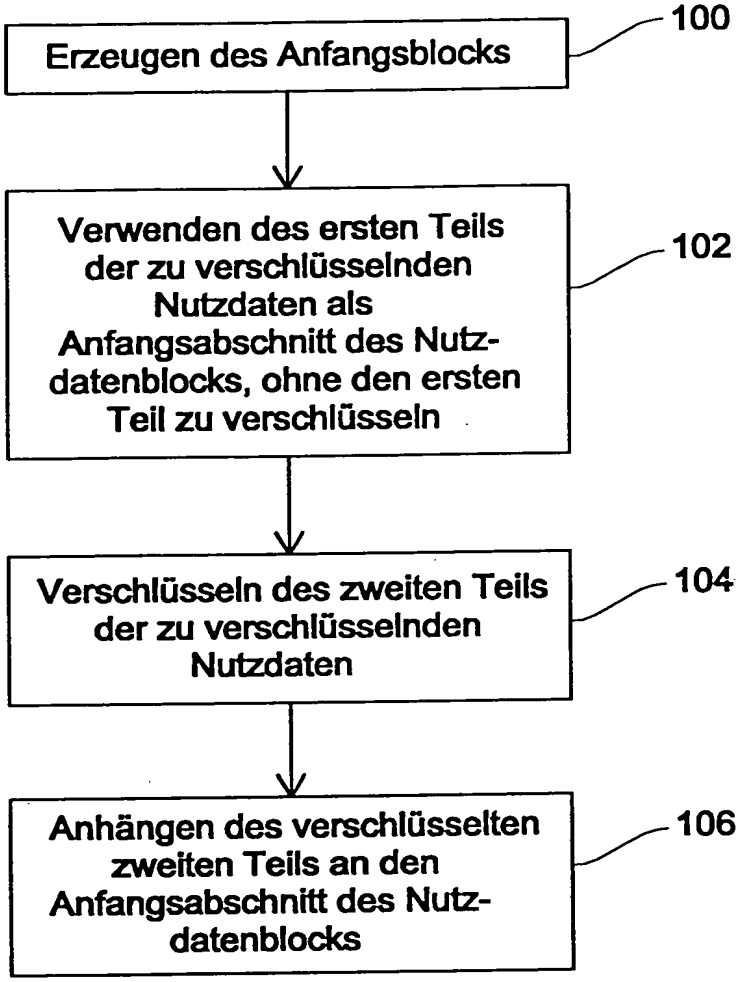
Erzeugen des Anfangsblocks
100
Verwenden des ersten Teils der zu verschlüsselnden Nutzdaten als Anfangsabschnitt des Nutzdatenblocks, ohne den ersten Teil zu verschlüsseln
102
Verschlüsseln des zweiten Teils der zu verschlüsselnden Nutzdaten
104
Anhängen des verschlüsselten zweiten Teils an den Anfangsabschnitt des Nutzdatenblocks
106

Fig. 4

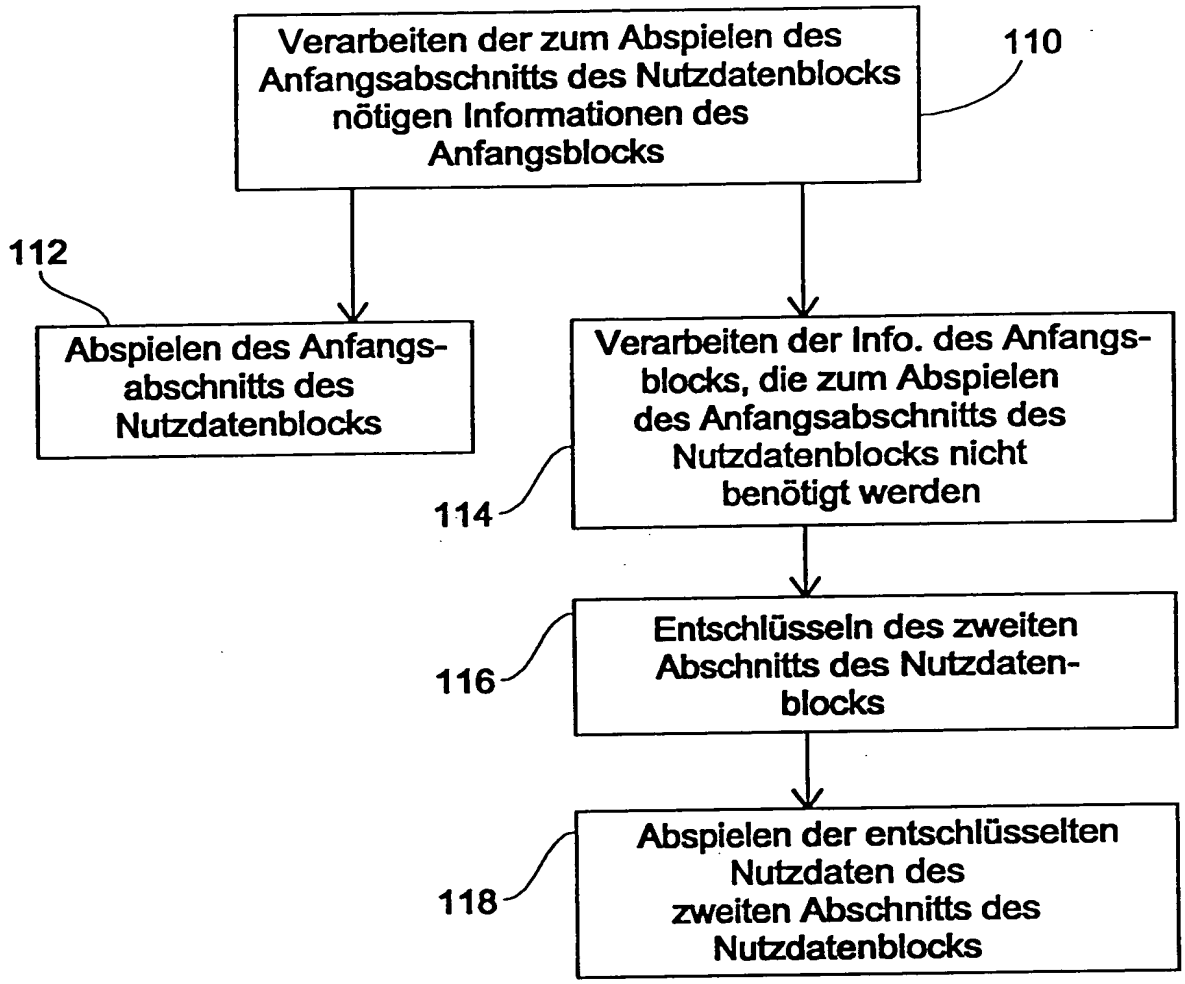
Verarbeiten der zum Abspielen des Anfangsabschnitts des Nutzdatenblocks nötigen Informationen des Anfangsblocks
110
112
Abspielen des Anfangs-abschnitts des Nutzdatenblocks
Verarbeiten der Info. des Anfangs-blocks, die zum Abspielen des Anfangsabschnitts des Nutzdatenblocks nicht benötigt werden
114
Entschlüsseln des zweiten Abschnitts des Nutzdaten-blocks
116
Abspielen der entschlüsselten Nutzdaten des zweiten Abschnitts des Nutzdatenblocks
118

Fig. 5

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF TRANSMITTAL OF COPIES OF TRANSLATION OF THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Rule 72.2)

To:

SCHOPPE, Fritz
Schoppe, Zimmermann & Stöckeler
Postfach 71 08 67
D-81458 München
ALLEMAGNE

Date of mailing (day/month/year) 31 August 2001 (31.08.01)	
Applicant's or agent's file reference FH991204.PCT	**IMPORTANT NOTIFICATION**
International application No. PCT/EP99/09977	**International filing date** (day/month/year) 15 December 1999 (15.12.99)
Applicant FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V. et al	

1. Transmittal of the translation to the applicant.

The International Bureau transmits herewith a copy of the English translation made by the International Bureau of the international preliminary examination report established by the International Preliminary Examining Authority.

2. Transmittal of the copy of the translation to the elected Offices.

The International Bureau notifies the applicant that copies of that translation have been transmitted to the following elected Offices requiring such translation:

JP,KR,US

The following elected Offices, having waived the requirement for such a transmittal at this time, will receive copies of that translation from the International Bureau only upon their request:

EP

3. Reminder regarding translation into (one of) the official language(s) of the elected Office(s).

The applicant is reminded that, where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report.

It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned (Rule 74.1). See Volume II of the PCT Applicant's Guide for further details.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer

Juan CRUZ

Telephone No. (41-22) 338.83.38

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference FH991204.PCT	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP99/09977	International filing date (*day/month/year*) 15 December 1999 (15.12.99)	Priority date (*day/month/year*) 16 February 1999 (16.02.99)
International Patent Classification (IPC) or national classification and IPC H04N 7/16, H04H 1/00		
Applicant FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
13 September 2000 (13.09.00)	17 November 2000 (17.11.2000)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/EP99/09977

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1-19, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____,
pages _____, filed with the letter of _____.

☒ the claims, Nos. 1-17, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. _____, filed with the letter of _____,
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1-4, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-17	YES
	Claims		NO
Inventive step (IS)	Claims	1-17	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-17	YES
	Claims		NO

2. Citations and explanations

1. PCT Article 33

1.1 Claim 1

The following documents are referred to:

D1: DE-C-196 25 635
D2: US-A-5 303 303

Document D1 is not cited in the international search report but is mentioned and summarised in the description (page 2).

According to D1 it was previously known to generate an encrypted multimedia data stream in which a destination data block (initial block or header) is followed by a user data block which is at least partially encrypted (see D1, Figure 3).

Claim 1 of the present application also provides for the generation of a header (initial block (12)). The position of the header in the data stream is not fixed, but it can also be at the beginning of the data stream, as is known from D1. This claimed feature is therefore not novel.

Document D2 (see the abstract and Figure 1) discloses a header at the beginning of a data stream and also another

header at the end of the data stream. A person skilled in the art would therefore be able to conclude that header information can be inserted not only at the beginning of a data stream but also in other positions in the data stream. To this extent the claimed feature could not be considered inventive even if it were novel over D1.

Claim 1 also provides for the generation of a user data block, as in D1 and D2. According to Claim 1, an encrypted second part of the user data block is preceded by an unencrypted first part. The object of the process in the context of the decryption of multimedia files is to be able to have a preview function and also to allow immediate playback with limited hardware requirements.

Thus the user data block according to Claim 1 is in effect only partially encrypted, as is known from D1. However, D1 does not disclose the possibility of having the unencrypted part precede the encrypted part. D1 merely proposes partial encryption and shows (Figure 3) the unencrypted part following the encrypted part.

In the light of the disclosure of D1, a person skilled in the art might consider arranging the two parts in the opposite order (unencrypted before encrypted), as claimed in the present application. However, there is nothing to specifically prompt him to change the order explicitly disclosed in D1. Moreover, the problem solved by the present invention is neither known from nor suggested by the available prior art.

Claim 1 is therefore considered to involve an inventive step and thus meets the requirements of PCT Article 33(2) and (3).

1.2 Claim 6

Claim 6 relates to the playing back of an encrypted multimedia data stream that can be generated by the process defined in Claim 1. The special process features defined in Claim 6 are as follows:

(a) the initial block data required in order to start playing the (unencrypted) initial portion of the user data block is processed;

(b) the unencrypted initial portion of the user data block is played back.

Neither of these features is known from or suggested by the prior art (D1 and D2).

Hence the requirements of PCT Article 33(2) and (3) are met.

1.3 Claims 12 and 13

Device Claims 12 and 13 correspond to Claims 1 and 6 and therefore also meet the requirements of PCT Article 33(2) and (3).

1.4

The invention is industrially applicable.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

2.1 The independent claims have not been drafted in the two-part form defined by PCT Rule 6.3(b). However, the two-part form does not seem to be appropriate in this case.

2.2 The word "*Viedeodaten*" (page 4, fifth paragraph, line 2) should read "*Videodaten*".